# On Some Applications of a Generalized Dwork Trace Formula to $L$-functions associated to Exponential Sums over Galois Rings

A DISSERTATION
SUBMITTED TO THE FACULTY OF THE GRADUATE
SCHOOL OF THE UNIVERSITY OF MINNESOTA
BY

Harris Ahmed Mohammed Ismail

IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Advisor: Dr. Steven Sperber

July, 2018

# Acknowledgements

First and foremost, I would like to thank my advisor, Dr. Steven Sperber, for introducing me to $p$-adic analisys and zeta functions - a beautiful area of mathematics, for teaching me the material with such fervour, for being very patient in explaining the nuances whenever I was confused, for patiently and carefully helping me get through the various difficulties I encounterd in my research by guiding me in the appropriate direction, for always encouraging me during my tough times, for taking the time to carefully read through my thesis drafts and suggesting revisions very promptly, especially, in the past few weeks, and for always believing in me.

Next, I would like to thank several professors in our Mathematics department for being very inspirational and influential. I would especially like to thank Dr. Paul Garrett and Dr. Ben Brubaker for their inspirational lectures in number theory, Dr. Peter Webb for his well-taught class in commutative and homological algebra, Dr. Kai-Wen Lan for his daunting, and yet, inspirational and very informative class in algebraic geometry, Dr. William Messing and Dr. Gennady Lyubeznik for their motivating classes in algebraic geometry, and Dr. Dihua Jiang for his informative class in automorphic forms that I very briefly attended. I would like to extend my special thanks to Dr. Victor Reiner for his prompt guidance on a combinatorial difficulty that I encountered in research. And I would like to thank Dr. Paul Garrett and Dr. Peter Webb once again for their valuable suggestions on improving my thesis draft. I would like to thank Dr. Prikry Karel, Dr. Dennis Hejhal and Dr. Bobbe Cooper for their exciting lectures in real analysis, complex analysis and algebra respectively, that drew me closer towards finding my passion in $p$-adic analysis. I extend my thanks to Prof. McGehee, Prof. Mosher, Bonny, Stephanie and Carla for always being friendly, kind and considerate and providing a great environment to work, thus helping me manage time between teaching and research better during the strenuous life at graduate school.

I would also like to thank all of my current colleagues at the University of Minnesota, Morris, especially, Ann Kolden, Carol Ford, Dr. Peh Ng, Dr. Mercredi Chasman, Dr. David Roberts, Dr. Barry McQuarrie, Dr. Chris Atkinson and Dr. Mark Logan for their timely help during a life threatening emergency that I had to encounter, a few months back. I thank them all again for accommodating me well at my new job with heavy teaching load by taking into consideration that I was also writing my dissertation simultaneously. I would like to thank Dr. Pieranna Garavaso for providing me with strong motivation for research through the exciting conversations we had. I would also like to thank Dr. John Kieffer, Dr. Nihar Jindal and Dr. Ahmed Tewfik who used to be

in our Electrical Engineering department for motivating me to pursue graduate studies in mathematics.

Next, I would like to thank "several" of my dear friends, who have been extremely helpful to me both by inspiring me and by personally encouraging me at tough times, every now and then. Without them, writing this dissertation would have been a million times more daunting. I would first like to thank my fellow math folks: Joe Dickinson (for all the inspiring intellectual discussions we had), Tuan Pham (for being a great close friend helping me in both math and non-math stuff), Po Hu (for being a good friend offering great suggestions), Heidi Anderson (for being a great friend during tough times; special thanks for proofreading my introduction carefully), Cihan Bahran (for inspiring me everytime), Emily Gunawan (for helping me a lot with job search), Heidi Goodson, Ali Adil, Adrienne Sands, Katie Storie, Ben Strasser, Cameron Thieme, Austin Tuttle, Jasper Weinburd, Nicole Brigland (special thanks for all the dissertation retreats we had), Shannon Negaard, Craig Corsi, Shelley Kandola, Ryan Goh, Jonas Karlsson, Shay and Kim Logan, Kate Meyer (for helping me a lot with job search by offering great suggestions), Maggie Ewing, David Morawski, Alex Fisher, Suma Karanam, Erin Manlove, Delia Samuel, Dennis Bashkirov, Julie Leifeld, Gabriella Jaramillo, Jessica Senou, Lauren Weum, Hania Pokora, Erin Oakley, Erin Stuhlsatz, Sam Fuller, Nur Saglam, Theo Douvropoulos, Doga Guctenkorkmaz, Vincent Quenneville-Bélair, Javier Acosta, Thomas McConville, Trevor Bain, Nicholas Switala and Xingjie Li. Next, I would like to thank my non-math friends, starting with my very close friends: Veena, Yash, Dwaipayan, Srujana (these four are very special to me for their constant motivation during tough times), Micah, Siddarth, Sharan, Gautham, Sandhya and Vijay, Nikhil (special thanks for inspiring me to become a great mathematician), GV, Amarthya, Vivek, Vincent, Shyam, Kalluri, Karthik, Abhishek (special thanks for all the enriching math conversations we had during dissertation retreat sessions), Tushar, Akshit, Subrahmaniam, Koko (special thanks for all the enjoyable math conversations we had), Joob, Nic, Yasir, Wendy, Srikrishnan, my Erie friends, my Bitsian friends, my high-school friends (most notably Alagan and Yoganeethi) and the list goes on. I would also like to thank some of my newer friends: Jennifer (special thanks to Jennifer for all the dissertation retreats we had, and for carefully checking for spelling/grammar/sylistic errors in my introduction), Emily (for offering great suggestions after reading my introduction chapter), Jayant and Afroz (for hosting me hospitably during the final stages in writing my dissertation) and Steven Morgan (for being a great friend).

Next, I would like to thank all of my inspirational teachers since elementary school through undergraduate college. I would specifically like to mention Ms. Raja Rajeshwari (Computer Science), Ms. Saira Banu (Mathematics), Ms. Dhamayanthi (Botany),

Mr. Nagarajan (Mathematics), Ms. Anitha (Physics), Prof. M. Ganesh (Mathematics) for inspiring me to become an academic in the sciences. I would also like to extend my special thanks to my dear friend Suri (Surendhaaren Venkatesan) for strongly inspiring me to become a pure mathematician when I was an undergraduate student in engineering, through our group-study sessions going over every single proof.

Next, I would like to thank my loving family and extended relatives - my parents for their constant support and encouragement, especially during all my tough times and for being with me at the final stages of my thesis revisions and degree completion; my dad for always enriching my aptitude for mathematics since childhood, and my mom for enriching my creativity and for always believing in me; my beloved brother, Wazim, for being with me always as my greatest friend-philosopher-guide, helping me daily during the toughest of my times, and inspiring me everytime.

Lastly, I want to thank all the students I had so far, for inspiring me to be a better mathematician with their curiosity to learn and fresh perspectives on everything I teach.

# Dedication

To my dearest brother, Wazim,

who rightly represents my loving family, and
all of my beloved friends and
inspirational teachers.

# Abstract

Dwork's trace formula is a seminal result proven by Bernard Dwork [Dwo60] (Section 2: Lemma 2), and it is one of the main ingredients in his celebrated proof of the rationality of the zeta function of an (affine or projective) algebraic variety over a finite field. In this thesis, we will prove a generalization of Dwork's trace formula that applies to exponential sums over Galois rings and the associated $L$-function. Using the generalized trace formula, we will prove more results on the $L$-function, analogous to the classical results by Dwork and Bombieri who studied $L$-functions associated to such exponential sums over finite fields. In particular, we will construct an analogue of the Dwork complex, and then prove the rationality of the $L$-function, and then obtain estimates on the degree (the number of zeros minus the number of poles) of the $L$-function (or its reciprocal) as in [Bom66] and the improvement by Adolphson and Sperber [AS87a]. We will conclude with a brief discussion on some interesting applications and extensions of this work that are worth investigating.

### To the reader who lacks sufficient mathematical background:

Finding integer solutions to polynomial equations (called as Diophantine problems) have been of great interest to humanity since antiquity. These fundamental problems have been driving significant developments in modern number theory and algebraic geometry. An algebraic variety is a geometric structure determined by the common zeros (solutions) to a system of polynomial equations. The zeta function of an algebraic variety encodes the information on the number of solutions to a system of polynomial equations in certain mathematical structures generalizing commonly used systems of numbers such as the integers, the rational numbers and the real numbers. More precisely, it encodes the sequence of the number of "rational points" on the variety. $L$-functions associated to exponential sums are related to the zeta function of an algebraic variety. This motivates the study of $L$-functions associated to exponential sums. On the other hand, exponential sums themselves are important objects of interest. For example, exponential sums like Gauss sums and Kloosterman sums play a fundamental role in analytic number theory. In general, the study of $L$-functions associated to exponential sums is of great interest due to the similarity with and the relationships to other $L$-functions and zeta functions all of which share important properties with the classical Riemann zeta function, the study of which has been of great interest for centuries for to its fundamental place in number theory.

# Contents

**Acknowledgements** **i**

**Dedication** **iv**

**Abstract** **v**

**List of Figures** **ix**

**Explanation of Notations** **x**

**1 Introduction** **1**

1.1 Outline . . . . . 1

1.2 The Weil Conjectures . . . . . 2

1.3 Galois Rings and our $L$-function in relation to the Weil Zeta Function . 4

1.4 Prior Related Work . . . . . 9

1.5 Rational Point Counts - A Motivating Application . . . . . 12

**2 A Review of Dwork's $p$-adic Theory in the context of certain Exponential Sums** **20**

2.1 A $p$-adic Analytic Expression for certain Exponential Sums . . . . . 21

2.1.1 The Artin-Hasse Series and Dwork's Splitting Functions . . . . . 21

2.1.2 Construction of Characters from Splitting Functions . . . . . 27

2.1.3 Sums of Characters constructed from Splitting Functions . . . . 37

2.2 The Trace Formula for the (base) case when $r = 1$ . . . . . 42

2.2.1 A Weight Function and certain $p$-adic Banach Spaces . . . . . 43
2.2.2 The Frobenius and the Trace Formula . . . . . 55
2.2.3 Realizing the Frobenius as a Chain Map on a Complex . . . . . 62

**3 A Generalized Dwork Trace Formula 75**

3.1 The Single Variable Case . . . . . 76
3.1.1 Monomial Vectors . . . . . 79
3.1.2 Growth of Coefficients of the Power Series associated to $\bar{f}$ . . . . 83
3.1.3 The case when $r = 2$ . . . . . 93
3.1.4 The case when $r = 3$ . . . . . 102
3.1.5 Alternate Approach . . . . . 106
3.2 The Multivariable Case . . . . . 122
3.2.1 The $\Lambda$-diagram Weight Function . . . . . 127
3.2.2 The $\Sigma$-diagram Weight Function . . . . . 133
3.2.3 The Generalized Dwork Trace Formula . . . . . 137

**4 The Dwork Complex 141**

4.1 The Generalized Dwork Trace Formula . . . . . 141
4.2 Realizing the Frobenius as a Chain Map on a Complex . . . . . 145

**5 Rationality and Bombieri-Adolphson-Sperber Bounds on the Degree 159**

5.1 Rationality of the $L$-function . . . . . 159
5.1.1 Theory of 0-Cycles for Affine Varieties over Galois Rings . . . . . 162
5.2 Bombieri-Adolphson-Sperber Bounds on the Degree of the $L$-function . 173
5.2.1 Proof of Theorem 5.2.6 . . . . . 185

**6 Conclusion and Future Directions 191**

6.1 Conclusion . . . . . 191
6.2 Future Directions . . . . . 193

6.2.1 Rational Point Counts . . . . . 193
6.2.2 $p$-divisibility of the Number of Solutions . . . . . 194
6.2.3 Formalism in terms of an Artin $L$-function . . . . . 195
6.2.4 Twisted Exponential Sums generalizing Gauss Sums . . . . . 196
6.2.5 Finite Dimensionality of the Cohomology of the Dwork Complex 197

**Bibliography** **198**

**Appendices** **202**

**A Hilbert's Theorem 90 for Galois Rings** **203**

**B Proofs of Some Basic Facts given in Chapter 2** **205**

B.1 Proof of Proposition 2.1.8 . . . . . 205
B.2 Proof of Corollary 2.1.10 . . . . . 206
B.3 Proof of Proposition 2.1.11 . . . . . 207
B.4 Proof of Lemma 2.1.12 . . . . . 208
B.5 Proof of Proposition 2.1.23 . . . . . 208
B.6 Proof of Lemma 2.2.3 . . . . . 209

**C Proof of Proposition 3.1.29 in Chapter 3** **211**

**D Proof of Equation 5.2.15 in Chapter 5** **216**

# List of Figures

1.1 Various Zeta Functions . . . . . 8

2.1 Action of the Dwork Frobenius on the Dwork Complex: $r = 1$ case . . . 73

3.1 The level-2 $\Delta$-diagram corresponding to $\bar{f}$ with $m = 4$ and $p = 5$ . . . . 96

3.2 The level-3 $\Delta$-diagram corresponding to $\bar{f}$ with $m = 2$ and $p = 3$ . . . . 105

3.3 The level-2 $\Lambda$-diagram corresponding to $\bar{f}$ with $m = 4$ and $p = 5$ . . . . 114

3.4 The level-3 $\Lambda$-diagram corresponding to $\bar{f}$ with $m = 2$ and $p = 3$ . . . . 114

4.1 Action of the Dwork Frobenius on the Dwork Complex: $r > 1$ case . . . 156

5.1 The level-2 $\Lambda$-diagram corresponding to $\bar{f}$ with $m = 4$ and $p = 5$ . . . . 186

# Explanation of Notations

## Frequently Used Variables

| | |
|---|---|
| $p$ | a fixed prime number |
| $a$ | a fixed positive integer |
| $q$ | the number $p^a$ |
| $r$ | a positive integer, either equalling 1 or greater than 1, inferred from the context |
| $l$ | a positive integer, usually indexing a sequence $\{S_l : l = 1, 2, ...\}$ of exponential sums |

## Frequently Used Sets

| | |
|---|---|
| $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ | integers, rational numbers, real numbers, complex numbers |
| $\mathbb{N}$ | positive integers (natural numbers) |
| $\mathbb{Z}_{>0}$, $\mathbb{Z}_{\geq 0}$ | positive integers, nonnegative integers |
| $\mathbb{Q}_{>0}$, $\mathbb{Q}_{\geq 0}$ | positive rational numbers, nonnegative rational numbers |
| $\mathbb{R}_{>0}$, $\mathbb{R}_{\geq 0}$ | positive real numbers, nonnegative real numbers |
| $\mathbb{F}_n$ | the finite field with $n$ elements; typically $n = p, p^j, q, q^l$ |
| $\mathbb{Q}_p$, $\mathbb{Z}_p$ | the $p$-adic numbers, the $p$-adic integers |
| $\mathbb{Q}_n$ | the unramified extension of $\mathbb{Q}_p$ of degree $\log_p n$; whenever $n = p, p^j, q, q^l$ |
| $\mathbb{Z}_n$ | the ring of integers of $\mathbb{Q}_n$; whenever $n = p, p^j, q, q^l$ |
| $\bar{\mathbb{Q}}$, $\bar{\mathbb{F}}_n$, $\bar{\mathbb{Q}}_n$ | algebraic closure of $\mathbb{Q}$, algebraic closure of $\mathbb{F}_n$, algebraic closure of $\mathbb{Q}_n$ |
| $\mathbb{Q}_n^{(u)}$ | the maximal unramified extension of $\mathbb{Q}_n$ in $\bar{\mathbb{Q}}_n$; whenever $n = p, p^j, q, q^l$ |
| $\mathbb{Z}_n^{(u)}$ | the ring of integers of $\mathbb{Q}_n^{(u)}$; whenever $n = p, p^j, q, q^l$ |
| $\mathbb{C}_p$ | completion of the algebraic closure of $\mathbb{Q}_p$ ($p$-adic complex numbers) |
| $\mathbb{Q}_v$, $\mathbb{Z}_v$, $\mathbb{C}_v$ | $v$-adic numbers, $v$-adic integers, $v$-adic complex numbers for a prime $v$ |
| $J_r$ | the set $\{0, 1, 2, ..., r-1\}$ |
| $GR(p^r, n)$ | the Galois ring of characteristic $p^r$ and degree $n$ over $\mathbb{Z}_p/p^r\mathbb{Z}_p$ (note that $GR(p^r, n)$ has cardinality $p^{nr}$) |
| $P$ | the ring $\mathbb{Z}_p/p^r\mathbb{Z}_p$, a construction of the Galois ring $GR(p^r, 1)$ |
| $R$ | the ring $\mathbb{Z}_q/p^r\mathbb{Z}_q$, a construction of the Galois ring $GR(p^r, a)$ |
| $R_l$ | the degree-$l$ Galois ring extension of $R$, namely, the ring $\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ |
| $\bar{R}$ | the ring $\mathbb{Z}_q^{(u)}/p^r\mathbb{Z}_q^{(u)}$ |

## Other Frequently Used Symbols

| | |
|---|---|
| $\mathrm{ord}_p$ | additive valuation on $\mathbb{C}_p$ normalized by $\mathrm{ord}_p\, p = 1$ |
| $\mathrm{ord}_q$ | additive valuation on $\mathbb{C}_p$ normalized by $\mathrm{ord}_q\, q = 1$ |
| $Gal(K/k)$ | the Galois group of a field extension $K$ of $k$, over $k$ (whenever $k$ is a field for which it makes sense) |
| $Gal(S/s)$ | the Galois group of a Galois ring extension $S$ of $s$, over $s$ (whenever $s$ is a Galois ring) |
| $\mathrm{Tr}_{K/k}$ | the *trace* map from a field extension $K$ of $k$, down to $k$ (whenever $k$ is a field for which it makes sense) |
| $\mathrm{Tr}_{S/s}$ | the *generalized trace* map from a Galois ring extension $S$ of $s$, down to $s$ (whenever $s$ is a Galois ring) |
| $\tau(q, l, r)$ | the generalized trace map $\mathrm{Tr}_{R_l/P}$ |
| $N_{K/k}$ | the *norm* map from a field extension $K$ of $k$, down to $k$ (whenever $k$ is a field for which it makes sense) |
| $\zeta_n$ | a primitive $n$-th root of unity; typically $n = p^r$ |
| $\Theta$ | an additive character of $\mathbb{F}_p$ into the field $\mathbb{Q}(\zeta_p)$ (for the most part, a nontrivial character of order $p$) |
| $\Theta^{(r)}$ | an additive character of $\mathbb{Z}_p/p^r\mathbb{Z}_p$ into the field $\mathbb{Q}(\zeta_{p^r})$ (for the most part, a nontrivial character of order $p^r$) |
| $E_p(t)$ | the Artin-Hasse exponential series, $\exp\left(\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^i}\right)$ |
| $\theta_\gamma(t)$ | $E_p(\gamma t)$ where $\gamma$ is a zero of $\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^i}$ |
| $\theta_j(t)$ | $\theta_{\gamma_j}(t)$ for each $j \in J_r$, where $\{\gamma_j : j \in J_r\}$ is a consistently chosen family of zeros of $\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^i}$ |
| $S_l(f), S_l^*(f)$, $S_l^{A,r}(f)$ | $l$-th element of various sequences of exponential sums associated to a polynomial $f$ (please use the context to identify the precise exponential sum that is being referred to) |
| $L(f,T), L^*(f,T)$ $L^{A,r}(f,T)$ | $L$-functions associated to various sequences of exponential sums associated to a polynomial $f$ (please use the context to identify the precise $L$-function that is being referred to) |

## More Symbols

| | |
|---|---|
| $\Delta_\infty(f)$ | Newton polyhedron of $f$ - defined in subsection 2.2.1 |
| $B_{\bar{f}}(b) = B_{\bar{f}}(b, K)$ | a $p$-adic Banach space associated to the polynomial $\bar{f}$ (first defined in subsection 2.2.1; also later in chapter 3 for a generalization) |
| $\psi_q, \psi_{q^l}$ | Dwork operator - first defined in subsection 2.2.2 (also later in chapter 4 for a generalization) |
| $\alpha$ | Dwork Frobenius operator - first defined in subsection 2.2.2 (also later in chapter 4 for a generalization) |
| $\alpha_0$ | an operator related to $\alpha$ - first defined in subsection 2.2.2 (also later in chapter 4 for a generalization) |
| $\sigma$ | usually refers to the Frobenius (generalized Frobenius) generator of a certain Galois group, inferred from the context |
| $L_i, L_{i,j}, \hat{L}_i$ | linear operators acting on certain $p$-adic Banach spaces (subsection 2.2.3, section 4.2) |
| $K^\bullet(\mathbf{L}, M)$ | the Dwork complex (subsection 2.2.3, section 4.2) |
| **Frob** | Dwork Frobenius map acting on $K^\bullet(\mathbf{L}, M)$ (subsection 2.2.3, section 4.2) |

## Some Symbols Defined In Chapter 3

| | |
|---|---|
| $I(\mu, r)$ | set of monomial vectors associated to the monomial $x^\mu$ |
| $M(\mu, r)$ | matrix representation of $I(\mu, r)$ |
| $I(\boldsymbol{\mu}, r)$ | set of monomial vectors associated to the monomial $\mathbf{x}^{\boldsymbol{\mu}}$ (the multivariable case) |
| $d(k), d(\mathbf{k})$ | exponent of $p$ associated to $k \in I(\mu, r)$, $\mathbf{k} \in I(\boldsymbol{\mu}, r)$ respectively |
| $K(\bar{f}, r)$ | a matrix associated to the polynomial $\bar{f}$ of degree $m$ (in one variable) |
| $K_\Delta(\bar{f}, r)$ | a matrix derived from $K(\bar{f}, r)$ |
| $K(\mu, r)$ | a matrix derived from $I(\mu, r)$ |
| $\underline{K}(\mu, r)$ | a matrix derived from $K(\mu, r)$ |
| $K(\boldsymbol{\mu}, r)$, $\underline{K}(\boldsymbol{\mu}, r)$ | multivariable analogues of $K(\mu, r)$, $\underline{K}(\mu, r)$ (derived from $I(\boldsymbol{\mu}, r)$) |
| $\Delta(\bar{f}, r)$ | the level-$r$ $\Delta$-diagram of the polynomial $\bar{f}$ |
| $\Lambda(\bar{f}, r)$ | the level-$r$ $\Lambda$-diagram of the polynomial $\bar{f}$ |
| $\Sigma(\bar{f}, r)$ | the level-$r$ $\Sigma$-diagram of the polynomial $\bar{f}$ |
| $w_\Delta, w_\Lambda, w_\Sigma$ | the $\Delta$, $\Lambda$, $\Sigma$ diagram weight functions respectively |

## Notes

1. In section 5.2, the symbol $R$ refers to the total number of zeros of the $L$-function, $L^*(\bar{f}, T)$ under consideration. Noting the fact that $\bar{f}$ is a polynomial over the Galois ring, $R = \mathbb{Z}_q/p^r\mathbb{Z}_q$, there is no need for any confusion, as the former $R$ is an integer counting the number of zeros, while the latter $R$ is a ring.

2. Apology: While I have tried my best in fixing typos and other unintentional errors, there may still be a few such errors here and there. I apologize for any inconvenience caused to the reader due to these errors.

*"It is impossible to be a mathematician without being a poet in soul."*

- Sofia Kovalevskaya [1850-1891]

*"Mathematics is the art of giving the same name to different things."*

- Henri Poincaré [1854-1912]

# Chapter 1

# Introduction

Dwork's $p$-adic theory has been seminal in the proof of the rationality of the zeta function of an algebraic variety ([Dwo60]) over a finite field, the first one of the Weil conjectures. One of the main tools in the development of Dwork's $p$-adic theory is the *Dwork trace formula* that relates certain exponential sums over finite fields with the trace of certain *completely continuous* endomorphisms [Ser62] over certain $p$-adic Banach spaces. In this thesis, we will investigate a generalization of the Dwork trace formula that applies to certain exponential sums over Galois rings (described later in this chapter) and present some applications of this generalized trace formula to the associated $L$-function.

## 1.1 Outline

In this chapter, we will first briefly quote the Weil conjectures that motivated the development of Dwork's $p$-adic theory and then describe the $L$-function that we consider in relation to the Weil zeta function and the related $L$-function, $L^*(T)$ studied by Dwork and Bombieri [Bom66]. We will then discuss the related work in the literature. Finally, we will discuss counting rational points in more detail, motivating the study of the exponential sums that we consider.

Chapter 2 is a review of the well-known essentials of Dwork's $p$-adic theory ([Dwo60],

[Dwo62]) and more specifically, the derivation of the Dwork trace formula and the construction of the Dwork complex. It includes improvements to the theory as studied independently by Adolphson and Sperber [AS87a], Blache [Bla03], and Liu and Wei [LW07]. In Chapter 3, we will prove a generalized Dwork trace formula that applies to the exponential sums that we consider. In Chapter 4, we will construct the analogue of the Dwork complex for the generalization. In Chapter 5, we will first prove that the associated $L$-funtion is rational and then prove the generalization of the Bombieri-Adolphson-Sperber bound for the degree of the $L$-function. In Chapter 6, we will conclude by discussing some applications and extensions of this work.

## 1.2 The Weil Conjectures

André Weil studied the number of solutions to a system of polynomial equations in finite fields in his remarkable paper in 1949 ([Wei49]). He defined the *Weil zeta function* and formulated the Weil conjectures. In this section, we will describe the Weil conjectures. Let $p$ be a prime number and let $q = p^a$ be a power of $p$ for some $a \geq 1$. Let $V$ be a smooth, projective algebraic variety of dimension $d$ over the finite field $\mathbb{F}_q$. The Weil zeta function associated to the variety[1], $V$ is defined as the formal power series

$$Z(V,T) = \exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right) \tag{1.2.1}$$

and where $N_s = N_s(V)$ is the number of $\mathbb{F}_{q^s}$-rational points of $V$. The statements of the Weil conjectures are as follows (We will state them as given in [Sil09].):

(i) $Z(V,T)$ is a rational function of $T$, i.e.,

$$Z(V,T) \in \mathbb{Q}(T)$$

[1]Please note that the original statements of the Weil conjectures were given for *projective* varieties. However, we study *affine* varieties in this work. Dwork's proof of rationality is valid for the zeta functions of both affine and projective varieties.

(ii) The zeta function satisfies a *functional equation* as follows: There is an integer $e$, called the Euler characteristic of $V$, such that

$$Z(V, q^{-d}T^{-1}) = \pm q^{\frac{de}{2}} T^e Z(V, T)$$

(iii) The zeta function satisfies an analogue of the *Riemann Hypothesis* as follows: The zeta function factors as

$$Z(V, T) = \frac{P_1(T)P_3(T)...P_{2d-1}(T)}{P_0(T)P_2(T)...P_{2d}(T)}$$

with each $P_i(T) \in \mathbb{Z}[T]$ with $P_0(T) = 1 - T$, $P_{2d}(T) = 1 - q^d T$ and for each $1 \leq i \leq 2d-1$, the polynomial $P_i(T)$ factors over $\bar{\mathbb{Q}}$, the field of algebraic numbers as $P_i(T) = \prod_{j=1}^{b_i} (1-\alpha_{ij}T)$ where $\alpha_{ij}$ are certain algebraic integers with their absolute values $|\alpha_{ij}| = q^{i/2}$. This implies that the zeros of the polynomial $P_i(T)$ viewed as a function of the complex variable $s$ via the change of variable, $T = q^{-s}$, have their real parts restricted to a critical line of complex numbers $s$ with real part $i/2$.

(iv) When the variety $V$ arises by reduction mod p of a variety, $\tilde{V}$, say defined over $\mathbb{Q}$ or a number field, the degree $b_i$ of the polynomial $P_i(T)$ is called the $i$-th *Betti number* of the variety $V$.

In 1960, Dwork [Dwo60] proved the rationality using methods of $p$-adic functional analysis. In 1965, Grothendeick proved the functional equation using $\ell$-adic cohomology theory and in 1974, Deligne proved the Riemann Hypothesis. In the subsequent chapters, we will describe the *Dwork trace formula* which is a key ingredient in Dwork's proof of the rationality of the zeta function. As pointed out earlier in the footnote, Dwork's proof of rationality is valid for zeta functions of both affine and projective varieties, and more generally for any variety of finite type.

A simple combinatorial argument using the orthogonality of characters (please see Section 1.5) relates the sequence of point counts $\{N_l : l = 1, 2, ...\}$ to an associated

sequence of character sums $\{S_l : l = 1, 2, ...\}$ and thus relates the zeta function with the $L$-function associated to the sequence of character sums. Each of the sums $S_l$ can be decomposed by a further combinatorial argument into a sequence of character sums of a different kind, $\{S_l^* : l = 1, 2, ...\}$ ([Dwo60], [Bom66]), which we will describe later in this chapter. Dwork relates such character sums, $S_l^*$ to the trace of completely continuous operators (the $p$-adic analogue of trace-class operators on spaces over Archimedean valued fields) on $p$-adic Banach spaces through his trace formula. The trace formula immediately gives striking results on the nature of the $L$-function, $\boxed{L^*(T) := \exp \sum_{l=1}^{\infty} \frac{S_l^* T^l}{l}}$ associated to the sequence of character sums of the second kind, $\{S_l^* : l = 1, 2, ...\}$. One can deduce the rationality and other properties of the zeta function by studying the properties of the $L$-function, $L^*(T)$.

## 1.3 Galois Rings and our $L$-function in relation to the Weil Zeta Function

In order to understand the $L$-function that we study, let us first review *Galois rings* briefly. These commutative rings (which generalize finite fields in a certain natural way, as we shall soon see) were first studied carefully by Wolfgang Krull in 1924. Later, Ernst Witt [Wit36] developed the theory of Witt vectors in 1936. It can be shown that Galois rings are isomorphic to the ring of Witt vectors of finite length over a finite field; please see [Rab14], [LW07] for an explicit isomorphim. A more comprehensive exposition of Galois rings can be found in [Wan03] or in [McD74].

**Definition 1.3.1.** A **Galois ring** is a finite ring with identity such that the set of its zero divisors along with 0 form a principal ideal $< p \cdot 1 >$ for some prime number $p$.

Let $p$ be a prime number and let $r$ and $a$ be positive integers. It can be shown that there is a unique Galois ring of characteristic $p^r$ and cardinality $p^{ra}$, and it is denoted by $GR(p^r, a)$. It can be shown that the Galois ring $GR(p^r, a)$ can be constructed in three ways as explained below.

Let $q = p^a$. Let $\mathbb{F}_p$ denote the finite field with $p$ elements, let $\mathbb{Q}_p$ denote the field

of $p$-adic numbers, let $\mathbb{Z}_p$ denote the ring of $p$-adic integers and let $W_r(\mathbb{F}_p)$ denote the ring of truncated Witt vectors of length $r$ over $\mathbb{F}_p$. For each integer $l$, let $\mathbb{F}_{p^l}$ denote the finite field with $p^l$ elements, let $\mathbb{Q}_{p^l}$ denote the unramified extension of degree $l$ over $\mathbb{Q}_p$, let $\mathbb{Z}_{p^l}$ denote the ring of integers in $\mathbb{Q}_{p^l}$ and let $W_r(\mathbb{F}_{p^l})$ denote the ring of truncated Witt vectors of length $r$ over $\mathbb{F}_{p^l}$. Then

(i) $\boxed{GR(p^r, a) \cong \frac{(\mathbb{Z}/p^r\mathbb{Z})[x]}{< h(x) >}}$, where $h(x)$ is a *monic basic irreducible* [Wan03] polynomial of degree $a$ over $\mathbb{Z}/p^r\mathbb{Z}$, that is, $h(x)$ a monic polynomial of degree $a$ in $(\mathbb{Z}/p^r\mathbb{Z})[x]$ whose reduction modulo $p$ is irreducible in $\mathbb{F}_p[x]$.

(ii) $\boxed{GR(p^r, a) \cong \mathbb{Z}_q/p^r\mathbb{Z}_q}$

(iii) $\boxed{GR(p^r, a) \cong W_r(\mathbb{F}_q)}$

and each $z \in GR(p^r, a)$ has a unique *additive representation*,

$$z = y_0 + y_1 t + y_2 t^2 + \ldots + y_{a-1} t^{a-1}$$

where $t$ is the root of the polynomial $h(x)$ which is adjoined to $(\mathbb{Z}/p^r\mathbb{Z})$ to form the ring $GR(p^r, a)$ and the digits $y_i$ belong to $(\mathbb{Z}/p^r\mathbb{Z})$,

and a unique *p-adic representation*,

$$z = x_0 + x_1 p + \ldots x_{r-1} p^{r-1}$$

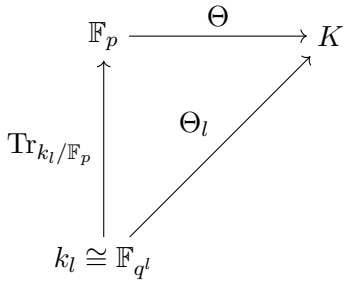
where the digits $x_i$ belong to the finite set of representatives called the set of *Teichmüller representatives*, $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{q-1}\}$ where $\xi$ is a primitive $(q-1)$-th root of unity. We will emphasize the second construction of Galois rings in our discussion.

Observe that for each integer $l$, $GR(p^r, al) \cong \mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$, and when $r = 1$, $GR(p, al) \cong \mathbb{F}_{q^l}$. And it can be shown that for integers $m, n$, $GR(p^r, m)$ contains a copy of $GR(p^r, n)$ if and only if $n|m$, and thus for integers $l$, the rings $GR(p^r, al)$ are all the finite ring extensions of $GR(p^r, a)$ in the same way as the fields $\mathbb{F}_{q^l}$ are all the finite field extensions of $\mathbb{F}_q$. The Frobenius endomorphisms on $\mathbb{F}_{q^l}$ with respect to $\mathbb{F}_q$, the trace maps $\mathrm{Tr}_{\mathbb{F}_{q^l}/\mathbb{F}_q}$ and

the norm maps $\mathrm{N}_{\mathbb{F}_{q^l}/\mathbb{F}_q}$ generalize respectively to generalized Frobenius endomorphisms on $GR(p^r, al)$ with respect to $GR(p^r, a)$, generalized trace maps $\mathrm{Tr}_{GR(p^r,al)/GR(p^r,a)}$ and generalized norm maps $\mathrm{N}_{GR(p^r,al)/GR(p^r,a)}$.

Now, let us understand our generalization in relation to the exponential sums and the associated $L$-function that Dwork originally studied.

1. **Dwork:** Let $k$ be a finite field with $q$ elements, so $k \cong \mathbb{F}_q$ and let $f(x)$ be a polynomial over $k$. For each integer $l$, let $k_l$ be the degree-$l$ extension of $k$. Let $K$ be the $p$-adic field $\mathbb{Q}_p(\zeta_p)$ where $\zeta_p$ is a primitive $p$-th root of unity. Let $\Theta$ be an additive character of $\mathbb{F}_p$ into $K$. Then, for each integer $l$, $\Theta_l := \Theta \circ \mathrm{Tr}_{k_l/\mathbb{F}_p}$ is an additive character of $k_l$ into $K$, and we have the following commutative diagram:




   Now, for each integer $l$, define

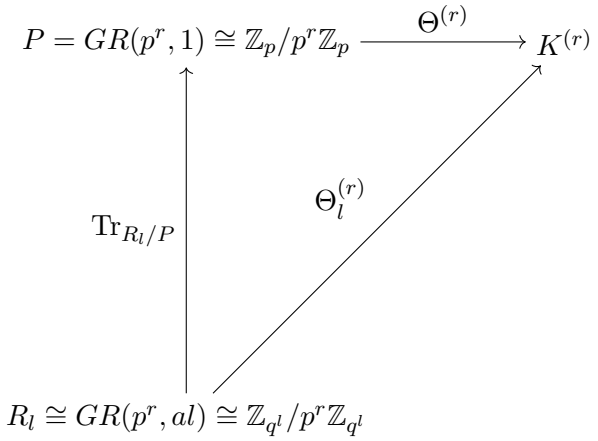
$$S_l^*(f) := \sum_{x \in k_l^*} \Theta_l(f(x))$$

   where $k_l^*$ is the set of all nonzero elements of $k_l$. Dwork studied these character sums and developed the Dwork Trace Formula that relates these sums to the trace of certain completely continuous endomorphisms on certain $p$-adic Banach spaces developed from $f(x)$. The associated $L$-function is given by

$$L^*(f, T) = \exp \sum_{l=1}^{\infty} \frac{S_l^*(f) T^l}{l}.$$

2. **Our Generaliztion:** Let $R$ be the Galois ring, $GR(p^r, a)$, and let $f(x)$ be a polynomial over $R$. For each integer $l$, let $R_l$ be the degree-$l$ extension of $R$, so

that $R_l \cong GR(p^r, al)$. Let $P$ be the Galois ring $GR(p^r, 1)$. Let $K^{(r)}$ be the $p$-adic field $\mathbb{Q}_p(\zeta_{p^r})$ where $\zeta_{p^r}$ is a primitive $p^r$-th root of unity. Let $\Theta^{(r)}$ be an additive character of $GR(p^r, a)$ into $K^{(r)}$. Then, for each integer $l$, $\Theta_l^{(r)} := \Theta \circ \mathrm{Tr}_{R_l/P}$ is an additive character of $R_l$ into $K^{(r)}$, and we have the following commutative diagram:




Now, note that each $x \in R_l$ has a $p$-adic representation

$$x = x_0 + x_1 p + x_2 p^2 + \ldots x_{r-1} p^{r-1}$$

where the digits $x_i$ belong to the finite set of *Teichmüller representatives*, $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{q-1}\}$ where $\xi$ is a primitive $(q^l - 1)$-th root of unity. Then for each $A \subseteq J_r := \{0, 1, 2, \ldots, r-1\}$, we may define the sets, $\mathcal{T}_l^{A,r}$ by

$$\mathcal{T}_l^{A,r} := \left\{ x = x_0 + x_1 p + ... + x_{r-1} p^{r-1} \in R_l : \begin{cases} x_i \neq 0, & \text{if } i \in A \\ x_i = 0, & \text{if } i \notin A \end{cases} \right\} \tag{1.3.1}$$

Now, for each $A \subset J_r$ and for each integer $l$, define

$$S_l^{A,r}(f) := \sum_{x \in \mathcal{T}_l^{A,r}} \Theta_l^{(r)}(f(x))$$

In this thesis, we will study the character sums $S_l^{A,r}(f)$ for the case when $\boxed{A = J_r = \{0, 1, 2, ..., r-1\}}$ and develop a generalized Dwork Trace Formula that relates these sums to the trace of certain completely continuous endomorphisms

on certain $p$-adic Banach spaces developed from $f(x)$ in an analogous way. The associated $L$-function is given by

$$L^{A,r}(f,T) = \exp \sum_{l=1}^{\infty} \frac{S_l^{A,r}(f)T^l}{l}.$$

We will prove the generalized trace formula for these sums in the multivariable case where $f(\mathbf{x})$ is a polynomial in $n$ variables $x_1, x_2, ..., x_n$. In that case, the sums generalize to $S_l^{A_1,A_2,...,A_n,r}$ where $A_1 = A_2 = \ldots = A_n = \{0, 1, 2, \ldots, r-1\}$.

We see that our generalization specializes to Dwork's case when $r = 1$ and $A = \{0\}$. A natural application of studying the sequence of sums $\{S_l^{(A_1,A_2,...,A_n),r}(f) : l = 1, 2, 3, ...\}$ in the multivariable case for all $A_i \subseteq J_r$ is counting the $R_l$-rational points of varieties over the Galois ring $R$ by using a character argument similar to that described in the previous section (please see Section 1.5 for more details). To better understand our $L$-function in relation to the Weil zeta function, it is useful to consider the following diagram.

$$\begin{array}{ccccccc}
\mathbb{F}_q \cong \mathbb{Z}_q/p\mathbb{Z}_q & \longrightarrow & \mathbb{F}_{q^2} \cong \mathbb{Z}_{q^2}/p\mathbb{Z}_{q^2} & \longrightarrow & \mathbb{F}_{q^3} \cong \mathbb{Z}_{q^3}/p\mathbb{Z}_{q^3} & \longrightarrow & ... \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathbb{Z}_q/p^2\mathbb{Z}_q & \longrightarrow & \mathbb{Z}_{q^2}/p^2\mathbb{Z}_{q^2} & \longrightarrow & \mathbb{Z}_{q^3}/p^2\mathbb{Z}_{q^3} & \longrightarrow & ... \\
\downarrow & & \downarrow & & \downarrow & & \\
\vdots & \longrightarrow & \vdots & \longrightarrow & \vdots & \longrightarrow & ... \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathbb{Z}_q/p^r\mathbb{Z}_q & \longrightarrow & \mathbb{Z}_{q^2}/p^r\mathbb{Z}_{q^2} & \longrightarrow & \mathbb{Z}_{q^3}/p^r\mathbb{Z}_{q^3} & \longrightarrow & ... \\
\downarrow & & \downarrow & & \downarrow & & \\
\vdots & \longrightarrow & \ddots & \longrightarrow & \ddots & \longrightarrow & ...
\end{array}$$

Figure 1.1: Various Zeta Functions

While the Weil zeta function and the related $L$-function, $L^*(T)$ studied by Dwork and

Bombieri corresponds to the first row in the above picture in the sense that the Weil zeta function counts the number of $\mathbb{F}_{q^l}$-rational points of a variety over $\mathbb{F}_q$, our $L$-function, $L^{(A_1,A_2,...,A_n),r}(T)$ with $A_i = J_r$ for all $i$ corresponds to the $r$-th row in the following sense. For simplicity let $V$ be a variety defined over $\mathbb{Z}$ and let $q = p$. Then it makes sense to view $V$ over $\mathbb{Z}_{p^l}$ and its reduction mod $p^r$. We may then count the number of $(\mathbb{Z}_{p^l}/p^r\mathbb{Z}_{p^l})$-rational points on $V \times \mathrm{Spec}(\mathbb{Z}_{p^l}/p^r\mathbb{Z}_{p^l})$ and form the usual generating series for fixed $r$ as $l$ varies. We will refer to this *zeta* function in Chapter 5 as we prove results on our $L$-function.

On the other hand, the Igusa zeta function ([Igu74], [DL98]), which counts the number of solutions of an equation modulo higher powers of $p$ corresponds to the first column in the above picture.

Diane Meuser [Meu86] considered a local zeta function in two variables that generalizes both the Weil zeta function and the Igusa zeta function. She proved the rationality of the zeta function that corresponds to the $r$-th row in the above picture. In this thesis, we will develop techniques based on Dwork's classical methods that provide an alternate proof for the rationality of the zeta function.

## 1.4 Prior Related Work

P.V. Kumar, Tor Helleseth and A. R. Calderbank [KHC95] studied sums of the form $S_l^{A,r}(f)$ and $S_l^{A,r}(f) + \Theta_l^{(r)}(0)$ for the case when $A = \{0\}$ where $f$ is a polynomial in a single variable. They proved an analogue of the Weil-Carlitz-Uchiyama bound for such exponential sums over Galois rings. The (Archimedean) bound finds immediate applications to coding theory.

Régis Blache [Bla03] studied exponential sums that looked like Gauss sums

$$G_{\mathcal{T}_a}(\Theta^{(r,a)}, \chi) := \sum_{x \in \mathcal{T}_a^*} \Theta^{(r,a)}(x)\chi(x)$$

where $\mathcal{T}_a := \mathcal{T}_a^* \cup \{0\}$, $\mathcal{T}_a^*$ is the set of Teichmüller units, $\{1, \xi, \xi^2, ..., \xi^{p^a-2}\}$ so that $\mathcal{T}_a$ is the set of Teichmüller representatives for the $p$-adic representation of elements

in $GR(p^r, a)$; $\Theta^{(r,a)}$ is an additive character of order $p^r$ over $\mathbb{Z}_{p^a}$ and thus an additive character of $GR(p^r, a)$ and $\chi$ is a multiplicative character of $\mathbb{Z}_{p^a}^*$ (the group of units of $\mathbb{Z}_{p^a}$) of order dividing $p^a - 1$. He called these *p-adic Gauss sums of level r* building up on the work of Langevin and Solé [LS00] who first studied these sums. Blache proved a generalization of the Stickelberger Theorem in this paper. His proof is based on his generalization of Dwork's theory of splitting of additive characters. Blache defines splitting functions of level $r$ and constructs a generalization of Dwork's splitting function based on the Artin-Hasse exponential series. We will discuss this in detail in Chapter 2. This result of his, Theorem 2.1.18, is crucial in the development of our generalized Dwork trace formula.

Later, Blache [Bla09] studied $L$-functions of exponential sums on smooth, projective curves over Galois rings. He considered sums of the form

$$S_l(C, f) := \sum_{\pi \in C_f(R_l)} \psi^{(l)}(f(\pi))$$

where $C$ is a smooth, projective curve over a Galois ring $R$, $R_l$ is the unramified extension of degee-$l$ of $R$, $\psi^{(l)} := \psi \circ \mathrm{Tr}_{R_l/R}$ where $\psi$ is an additive character of $R$ of order $p^r$, $f$ is a function over $C$, $C_f(R_l)$ is the set of all $R_l$-rational points of $C$ at which $f$ is defined. He proved the rationality of the associated $L$-function using the properties of the Greenberg functor and with the Lefshetz-Grothendeick trace formula and $\ell$-adic étale cohomology theory (where $\ell$ is a prime different from $p$). However, he did not develop the analogue of a Dwork trace formula in this case. The Dwork trace formula would provide another proof of the rationality using Dwork's $p$-adic theory.

More recently, Sandi Xhumari [Xhu16] proved a generalized Dwork Trace Formula for a generalized $p$-adic Gauss sum that generalizes the sum $S_l^{\{0\},r}(f)$ in the special case when $f(x) = ux$ where $u$ is a unit in $GR(p^r, a)$. More precisely, he considered sums of the form

$$-\sum_{t \in \mu_{q-1}} t^{-s} \zeta_{p^r}^{\mathrm{Tr}(t\nu)}$$

where $\mu_{q-1}$ is the set of $(q-1)$-th roots of unity, $0 \leq s \leq (q-2)$ and $\nu \in (\mathbb{Z}_q/p^r\mathbb{Z}_q)^\times$, and obtained a Dwork Trace Formula for these sums. He used it to prove a generalized

Gross-Koblitz formula.

Chunlei Liu and Dasheng Wei [LW07] studied $L$-functions of Witt coverings and developed an analogue of Dwork's $p$-adic theory and a trace formula for the associated exponential sums which are related to exponential sums of the form $S_l^{A,r}$ with $A = \{0\}$ for $l = 1, 2, ....$ The exponential sums they considered apply to a Laurent polynomial $f(x) \in GR(p^r, a)[x_1^{\pm 1}, x_2^{\pm 1}, ..., x_n^{\pm 1}]$. They proved a generalization of Bombieri-Adolphson-Sperber bound for the total degree (the total number of zeros and poles) of such $L$-functions. We shall prove such a generalization of Bombieri-Adolphson-Sperber bound on the degree (the number of zeros minus the number of poles) of the $L$-function associated to the sum $S_l^{A,r}$ with $A = J_r = \{0, 1, 2, ..., r-1\}$, (or its reciprocal), in this thesis.

Chunlei Liu and Daqing Wan [LW09] later introduced $T$-adic exponential sums of a Laurent polynomial $f(x) \in \mathbb{Z}_q[x_1^{\pm 1}, x_2^{\pm 1}, ..., x_n^{\pm 1}]$ defined as

$$S_l(f, T) := \sum_{x \in \mu_{q^l-1}^n} (1+T)^{\mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(f(x))} \in \mathbb{Z}_p[[T]]$$

where $\mu_{q^l-1}$ is the set of all $(q^l - 1)$-th roots of unity, and the associated $L$-function of $f$ over $\mathbb{F}_q$ as the generating function,

$$L(f, T, s) = L(f, T, s; \mathbb{F}_q) = \exp \sum_{l=1}^{\infty} S_l(f, T) \frac{s^l}{l} \in 1 + s\mathbb{Z}_p[[T]][[s]].$$

These exponential sums interpolate classical exponential sums of $p^r$-order over finite fields for all positive integers $r$. Substituting $T = 1 - \Theta^{(r)}(1)$, we get that

$$S_l(f, T) = S_l^{\{0\},r}(f)$$

in the case when $f$ is a polynomial over $GR(p^r, a)$ for example. The $T$ thus generalizes the uniformizer $(1 - \Theta^{(r)}(1))$. They prove a generalization of Dwork's $p$-adic theory and trace formula to the $T$-adic $L$-function to prove that the $L$-function is $T$-adic meromorphic, and later obtain estimates for the $T$-adic Newton polygon of the $C$-function associated to the $L$-function.

## 1.5 Rational Point Counts - A Motivating Application

In this section, we will discuss the usefulness of exponential sums in counting rational points of varieties and motivate the study of the exponential sums that we consider by presenting a similar application in the context of Galois rings.

### The Finite Field Case

Fix a primitive $p$-th root of unity, $\zeta_p$. Let $K = \mathbb{Q}_p(\zeta_p)$. Let $\Theta$ be an additive character of $\mathbb{F}_p$ into $K$. Note that $\Theta$ maps into $\mu_p(K)$, the multiplicative group of $p$-th roots of unity. Then, for each positive integer $s$, the composite $\Theta_{q^s} := \Theta \circ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ defines an additive character of $\mathbb{F}_{q^s}$ into $K$, where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ and $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ denote the trace maps.

Let $V$ be an *affine* algebraic variety over $\mathbb{F}_q$ defined by a set of $m$ polynomial equations in $n$ variables:

$$f_i(x) := f_i(x_1, x_2, ..., x_n) = 0 \qquad\qquad i = 1, 2, ..., m$$

where the polynomials, $f_i(x) \in \mathbb{F}_q[x_1, x_2, ..., x_n]$. And let $N_s$ denote the number of $\mathbb{F}_{q^s}$-rational points of $V$.

**Definition 1.5.1.** For each positive integer $s$, we define *the character sum at level $s$ associated to $V$* and the character $\Theta$ as follows:

$$\tilde{S}_s(\Theta, V, \mathbb{F}_{q^s}^{n+m}) := \sum \Theta_{q^s}\left(\sum_{i=1}^{m} y_i f_i(x)\right) \tag{1.5.1}$$

where the outer sum runs over all $m$-uples $y = (y_1, y_2, ..., y_m) \in \mathbb{F}_{q^s}^m$ and all $n$-uples $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_{q^s}^n$.

**Proposition 1.5.2.** *Let $s$ be a positive integer and let $\Theta$ be a nontrivial additive character of $\mathbb{F}_p$ into $K$. Then $\Theta_{q^s}$ is a nontrivial additive character of $\mathbb{F}_{q^s}$ and*

$$\tilde{S}_s(\Theta, V, \mathbb{F}_{q^s}^{n+m}) = q^{ms} N_s$$

*Proof.* We first observe that since $\Theta$ is a nontrivial character of order $p$, so is $\Theta_{q^s}$ because the trace map $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$ is surjective. (The polynomial $x + x^p + x^{p^2} + ... + x^{q^s/p}$ has at most $q^s/p$ zeros and hence the trace map is nontrivial. More generally, the trace map of any finite, separable extension is nontrivial [Lan05]. Thus, the nontrivial image of the trace map being an $\mathbb{F}_p$-subspace of $\mathbb{F}_p$ must coincide with $\mathbb{F}_p$). Now since $\Theta_{q^s}$ is a *nontrivial* character, we have that

$$\sum_{z \in \mathbb{F}_{q^s}} \Theta_{q^s}(z) = 0 \qquad (\star)$$

Now let $x \in \mathbb{F}_{q^s}^n$. Then we have

$$\begin{aligned}
\sum_{y \in \mathbb{F}_{q^s}^m} \Theta_{q^s}\left(\sum_{i=1}^m y_i f_i(x)\right) &= \sum_{y \in \mathbb{F}_{q^s}^m} \prod_{i=1}^m \Theta_{q^s}\left(y_i f_i(x)\right) \\
&= \prod_{i=1}^m \sum_{y_i \in \mathbb{F}_{q^s}} \Theta_{q^s}\left(y_i f_i(x)\right) \\
&= \begin{cases} \prod_{i=1}^m 0 & \text{if } f_i(x) \neq 0 \text{ for some } i \\ \prod_{i=1}^m q^s & \text{if } f_i(x) = 0 \text{ for all } i \end{cases} \\
&= \begin{cases} 0 & \text{if } x \text{ is not an } \mathbb{F}_{q^s}\text{-rational point of } V \\ q^{ms} & \text{if } x \text{ is an } \mathbb{F}_{q^s}\text{-rational point of } V \end{cases}
\end{aligned}$$

Therefore, we have that

$$\begin{aligned}
\tilde{S}_s(\Theta, V, \mathbb{F}_{q^s}^{n+m}) &= \sum_{x \in \mathbb{F}_{q^s}^n} \sum_{y \in \mathbb{F}_{q^s}^m} \Theta_{q^s}\left(\sum_{i=1}^m y_i f_i(x)\right) \\
&= q^{ms} N_s
\end{aligned}$$

□

Let us now define *affine* exponential sums associated to a polynomial and establish the connection between these exponential sums and the zeta function, $Z(V,T)$ of the affine algebraic variety, $V$ in more explicit terms.

**Definition 1.5.3.** For a polynomial, $f(x) \in \mathbb{F}_q[x_1, x_2, ..., x_N]$ in $N$ variables, define the family of exponential sums, $\{S_l(\Theta, f) : l \geq 1\}$ associated to the character $\Theta$ by

$$S_l = S_l(\Theta, f) = S_l(\Theta, f, \mathbb{A}^N(\mathbb{F}_q)) := \sum_{x \in \mathbb{F}_{q^l}^N} \Theta \circ \mathrm{Tr}_{\mathbb{F}_{q^l}/\mathbb{F}_p}(f(x))$$

where $\mathbb{A}^N(\mathbb{F}_q)$ is the affine $N$-space over $\mathbb{F}_q$. Then we define the $L$-function associated to this family of exponential sums as follows:

$$L(\Theta, f, \mathbb{A}^N(\mathbb{F}_q), T) := \exp\left(\sum_{l=1}^{\infty} \frac{S_l T^l}{l}\right).$$

Now, let $g_V(x, y) := \sum_{i=1}^{m} y_i f_i(x) \in \mathbb{F}_q[y_1, y_2, ..., y_m, x_1, x_2, ..., x_n]$. Then, for $N = n + m$, for each integer $l$, we see that the exponential sum,

$$S_l(\Theta, g_V) = \tilde{S}_l(\Theta, V, \mathbb{F}_{q^s}^{n+m})$$

From Proposition 1.5.2, we immediately deduce that the zeta function, $Z(V, T) = L(\Theta, g_V, \mathbb{A}^{n+m}(\mathbb{F}_q), q^m T)$ and in particular, $Z(V, T)$ is rational if and only if the $L$-function, $L(\Theta, g_V, \mathbb{A}^n(\mathbb{F}_q), T)$ is rational.

Thus the sums $S_l(\Theta, f)$ are useful. In Dwork's $p$-adic theory, however, a sequence of a different kind of exponential sums is the more natural object.

**Definition 1.5.4.** For a polynomial, $f(x) \in \mathbb{F}_q[x_1, x_2, ..., x_N]$ in $N$ variables, define the family of *toric* exponential sums, $\{S_l^*(\Theta, f) : l \geq 1\}$ associated to the character $\Theta$ by

$$S_l^* = S_l^*(\Theta, f) = S_l^*(\Theta, f, \mathbb{G}_m^N(\mathbb{F}_q)) := \sum_{x \in (\mathbb{F}_{q^l}^\times)^N} \Theta \circ \mathrm{Tr}_{\mathbb{F}_{q^l}/\mathbb{F}_p}(f(x))$$

where $\mathbb{G}_m^N$ is the $N$-dimensional torus over $\mathbb{F}_q$, and $\mathbb{F}_{q^l}^\times$ is the multiplicative group of $\mathbb{F}_q$ (and thus $\mathbb{G}_m = \mathbb{F}_q^\times$). Then we define the $L$-function associated to this family of

exponential sums as follows:

$$L^*(\Theta, f, \mathbb{G}_m^N(\mathbb{F}_q), T) := \exp\left(\sum_{l=1}^{\infty} \frac{S_l^* T^l}{l}\right)$$

There is a simple combinatorial relationship [Bom66] between sums of the kind $S_l$ and those of the kind $S_l^*$. Using

$$S_l(f) = \sum_A S_l^*(f_A)$$

where $A$ is any subset (including the empty set) of $\{1, 2, ..., N\}$ and $f_A$ is the polynomial in $N - \text{card}(A)$ variables obtained from $f$ by setting $x_i = 0$ for $i \in A$, we see that the sums $S_l^*$ are useful in computing rational point counts.

This motivates us to study sums of the kind $S_l^*$ and its generalizations. To understand the usefulness of the generalization that we consider, let us now describe rational point counts of varieties over Galois rings in terms of sums of this kind.

### Generalization to Galois Rings

Fix a positive integer $r$. Let $P$ be the Galois ring $GR(p^r, 1)$. Let $R$ be the Galois ring $GR(p^r, a)$ and for each integer $l$, let $R_l$ be the degree-$l$ extension of $R$. For simplicity, let $h(x) \in R[x]$ be a polynomial in a single variable $x$. Define $\boxed{g_h(x, y) := yh(x)}$. Let $K = \mathbb{Q}_p(\zeta_{p^r})$ for a fixed primitive $p^r$-th root of unity, $\zeta_{p^r}$. Let $\Theta^{(r)}$ be a nontrivial additive character of $P$ into $K$. Then for each $l$, $\Theta_l^{(r)} := \Theta^{(r)} \circ \text{Tr}_{R_l/R}$ is a nontrivial additive character of $R_l$ (please see Proposition 1.5.6 below). Let us now define the analogous character sums $S_l$ and the analogues of $S_l^*$ as introduced in Section 1.3.

**Definition 1.5.5.** For a polynomial, $f(x) \in R[x_1, x_2, ..., x_n]$ in $n$ variables, define the family of exponential sums, $\{S_l(\Theta^{(r)}, f) : l \geq 1\}$ associated to the character $\Theta^{(r)}$ by

$$S_l = S_l(\Theta^{(r)}, f, r) = S_l(\Theta^{(r)}, f, r, \mathbb{A}^n(R)) := \sum_{x \in R_l^n} \Theta^{(r)} \circ \mathrm{Tr}_{R_l/P}(f(x))$$

where $\mathbb{A}^n(R)$ is the affine $n$-space over the ring $R$. Then we define the $L$-function associated to this family of exponential sums as follows:

$$L(\Theta^{(r)}, f, r, \mathbb{A}^n(R), T) := \exp\left(\sum_{l=1}^{\infty} \frac{S_l T^l}{l}\right).$$

Now, for each subset $A_i \subseteq J_r := \{0, 1, 2, ..., r-1\}, i = 1, 2, ..., n$ and each integer $l$, define the sum, $S_l^{(A_1, A_2, ..., A_N), r}$ by

$$\begin{aligned} S_l^{(A_1, A_2, ..., A_n), r} &= S_l^{(A_1, A_2, ..., A_n), r}(\Theta^{(r)}, f, r, \mathcal{T}^{(A_1, A_2, ..., A_n), r}) \\ &:= \sum_{x \in \mathcal{T}_l^{(A_1, A_2, ..., A_n), r}} \Theta^{(r)} \circ \mathrm{Tr}_{R_l/P}(f(x)) \end{aligned}$$

where

$$\mathcal{T}_l^{(A_1, A_2, ..., A_n), r} := \prod_{i=1}^{n} \mathcal{T}_l^{A_i, r}$$

where the factors $\mathcal{T}_l^{A_i, r}$ are as defined in equation 1.3.1 in Section 1.3, that is,

$$\mathcal{T}_l^{A_i, r} := \left\{ x = x_0 + x_1 p + ... + x_{r-1} p^{r-1} \in R_l : \begin{cases} x_j \neq 0, & \text{if } j \in A_i \\ x_j = 0, & \text{if } j \notin A_i \end{cases} \right\},$$

and $\mathcal{T}^{(A_1, A_2, ..., A_n), r} := \mathcal{T}_1^{(A_1, A_2, ..., A_n), r}$.

The associated $L$-function is defined analogously as

$$L^{(A_1, A_2, ..., A_n), r}(\Theta^{(r)}, f, r, \mathcal{T}^{(A_1, A_2, ..., A_n), r}, T) := \exp\left(\sum_{l=1}^{\infty} \frac{S_l^{(A_1, A_2, ..., A_n), r} T^l}{l}\right).$$

Observe that for the two-variable case when $f(x,y) = g_h(x,y) = yh(x)$,

$$S_l^{(A_1,A_2),r}(\Theta^{(r)}, g_h, r, \mathcal{T}^{(A_1,A_2),r}) := \sum_{\substack{x\in\mathcal{T}_l^{A_1,r}\\ y\in\mathcal{T}_l^{A_2,r}}} \Theta^{(r)} \circ \mathrm{Tr}_{R_l/P}(yh(x)).$$

As with the finite field case, we have the following proposition.

**Proposition 1.5.6.** *If $\Theta^{(r)}$ is a nontrivial additive character of order $p^r$ of $P := GR(p^r,1)$, then for every positive integer $l$, the character $\Theta_l^{(r)} := \Theta^{(r)} \circ \mathrm{Tr}_{R_l/P}$ of $R_l$ is also nontrivial and of order $p^r$ and for $w \in R_l$, we have*

$$\sum_{y\in R_l} \Theta_l^{(r)}(yw) = \begin{cases} q^{lr} & \text{if } w = 0 \\ 0 & \text{if } w \neq 0 \end{cases}$$

*Proof.* That $\Theta_l^{(r)}$ is nontrivial and is of order $p^r$ is not hard to see. The classical Hilbert's Theorem 90 for finite fields generalizes to Galois rings, and from that it easily follows that the trace map $\mathrm{Tr}_{R_l/P}$ is surjective. (Please see Appendix A for a full proof of this fact).

Now, if $w = 0$, the sum is clearly $q^{lr}$. If $w \neq 0$, consider two cases. If $w$ is a unit, then $\{yw : y \in R_l\} = R_l$ and hence the sum is 0 since $\Theta_l^{(r)}$ is nontrivial. If $w \neq 0$ and $w$ is not a unit, then $w = p^k u$ for some unit $u \in R_l$ and some $k \in \{1, 2, ..., r-1\}$. Then

$$\begin{aligned}
\sum_{y\in R_l} \Theta_l^{(r)}(yw) &= \sum_{y\in R_l} \Theta_l^{(r)}(p^k yu) \\
&= \sum_{y\in R_l} \Theta_l^{(r)}(p^k y) \\
&= \sum_{\substack{y_i^{q^l}=y_i \\ 0\le i\le r-1}} \Theta_l^{(r)}(p^k(y_0 + y_1 p + \ldots + y_{r-1}p^{r-1})) \\
&= (q^l)^k \sum_{\substack{y_i^{q^l}=y_i \\ 0\le i\le r-1-k}} \Theta_l^{(r)}(p^k(y_0 + y_1 p + \ldots + y_{r-1-k}p^{r-1-k}))
\end{aligned}$$

$$
\begin{aligned}
&= q^{lk} \sum_{\substack{y_i^{q^l}=y_i \\ 0\le i\le r-1-k}} \Theta^{(r)} \circ \mathrm{Tr}_{R_l/P}\left[p^k(y_0+y_1p+\ldots+y_{r-1-k}p^{r-1-k})\right] \\
&= q^{lk} \sum_{\substack{y_i^{q^l}=y_i \\ 0\le i\le r-1-k}} \Theta^{(r)}\left[p^k \,\mathrm{Tr}_{R_l/P}(y_0+y_1p+\ldots+y_{r-1-k}p^{r-1-k})\right] \\
&= q^{lk} \sum_{y\in GR(p^{r-k},a)} \Theta^{(r)}\left[p^k \,\mathrm{Tr}_{R_l/P}(y_0+y_1p+\ldots+y_{r-1-k}p^{r-1-k})\right] \\
&= q^{lk} \sum_{y\in GR(p^{r-k},a)} \Theta^{(r)}(1)^{p^k \,\mathrm{Tr}_{R_l/P}(y_0+y_1p+\ldots+y_{r-1-k}p^{r-1-k})} \\
&= q^{lk} \sum_{y\in GR(p^{r-k},a)} \Theta^{(r-k)}(1)^{\mathrm{Tr}_{GR(p^{r-k},a)/GR(p^{r-k},1)}(y_0+y_1p+\ldots+y_{r-1-k}p^{r-1-k})}
\end{aligned}
$$

where $\Theta^{(r-k)}$ defined by $\Theta^{(r-k)}(1) = \Theta^{(r)}(1)^{p^k}$ is a nontrivial character of $GR(p^{r-k},a)$ of order $p^{r-k}$. And thus,

$$
\begin{aligned}
\sum_{y\in R_l} \Theta_l^{(r)}(yw) &= q^{lk} \sum_{z\in GR(p^{r-k},a)} \Theta^{(r-k)} \circ \mathrm{Tr}_{GR(p^{r-k},a)/GR(p^{r-k},1)}(z) \\
&= 0.
\end{aligned}
$$

□

From Proposition 1.5.6, we immediately deduce

**Proposition 1.5.7.** *Let $N_l$ be the number of solutions to $h(x)=0$ in the ring $R_l$. Then*

$$S_l(\Theta^{(r)}, g_h, r) = S_l(\Theta^{(r)}, yh(x), r) = q^{lr}N_l.$$

This motivates us to study sums of the kind $S_l(f,\Theta^{(r)},r)$ described above. Now, we may combinatorially decompose these sums as follows, as in [Bom66].

A polynomial $f\in R[x_1,x_2,...,x_n]$ may be considered as a polynomial in $nr$ variables $x_{i,j}$ by considering for each $i=1,2,...,n$, the $p$-adic expansion of the variable $x_i$ given by

$$x_i = x_{i,0} + x_{i,1}p + ... + x_{i,r-1}p^{r-1}.$$

Then, by an obvious combinatorial argument, we have

$$S_l(\Theta^{(r)}, f, r) = \sum_{\substack{A_i \subseteq J_r \\ 1 \leq i \leq n}} S_l^{(A_1, A_2, \ldots, A_n), r}(\Theta^{(r)}, f, r, \mathcal{T}^{(A_1, A_2, \ldots, A_n), r}).$$

We are thus motivated to study sums of the kind $S_l^{(A_1, A_2, \ldots, A_n), r}$. As mentioned earlier, in this thesis we will study sums of the kind $S_l^{(J_r, J_r, \ldots, J_r), r}$. To avoid this cumbersome notation, we will from now on use $S_l^*$ (analogous to Dwork's $S_l^*$; please see Chapter 2: subsection 2.1.3) to denote the generalized sums of this kind.

---

Before moving on to the next chapter, let us fix certain notations which do not change in any of the subsequent chapters in this thesis. We fix a prime number, $p$ and fix a positive integer, $a$ and let $q = p^a$. Let $\mathbb{C}_p$ denote the completion of an algebraic closure of $\mathbb{Q}_p$, the field of $p$-adic numbers, and let $\mathrm{ord}_p$ denote the additive valuation on $\mathbb{C}_p$ normalized by $\mathrm{ord}_p\, p = 1$. The field $\mathbb{C}_p$ (like $\mathbb{C}$ itself) is a good field to do analysis over since it is both complete and algebraically closed. We consider all our $p$-adic fields to be embedded in $\mathbb{C}_p$.

# Chapter 2

# A Review of Dwork's $p$-adic Theory in the context of certain Exponential Sums

In this chapter, we will review the essentials of Dwork's $p$-adic theory ([Dwo60], [Dwo62]) including the generalizations by Blache [Bla03], Liu and Wei [LW07] and Adolphson and Sperber [AS87a]. In Section 1, we will obtain a $p$-adic analytic expression for the character sums studied by Dwork. We will also introduce the character sums that generalize Dwork's character sums as described in the introduction. In Section 2, we will develop the basic Dwork trace formula and then use it to build the associated Dwork complex.

## 2.1 A $p$-adic Analytic Expression for certain Exponential Sums

### 2.1.1 The Artin-Hasse Series and Dwork's Splitting Functions

The Artin-Hasse exponential series, $E_p(t)$ corresponding to the prime number, $p$ is defined as the formal power series,

$$E_p(t) = \exp\left(\sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}\right) = \prod_{j=0}^{\infty} \exp\left(\frac{t^{p^j}}{p^j}\right)$$

It can be shown that the Artin-Hasse exponential series, $E_p(t)$ corresponding to the prime number, $p$ has coefficients which are not only rational numbers but are also $p$-adic integers, that is, $E_p(t) \in (\mathbb{Q} \cap \mathbb{Z}_p)[[t]]$. (This is an easy consequence of Dwork's Integrality Lemma, a version of it is stated as Lemma 3 in ([Kob84], Chapter IV: Section 2)). Looking at $E_p(t)$ as an $\mathbb{C}_p$-valued function, we can talk about the convergence of this power series and in fact, $E_p(t)$ has interesting $p$-adic analytic properties. As a consequence of these properties, we can derive an important result which motivates the definition of Dwork's *splitting functions*, later generalized to *splitting functions at level* $r$ by Blache [Bla03]. The main goal of this subsection is to prove this important result and define the splitting functions.

**Theorem 2.1.1.** *Let* $S(t) := \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$. *Let* $r$ *be a positive integer. Let* $\gamma$ *be a zero of* $S(t)$ *satisfying* $\operatorname{ord}_p \gamma = \dfrac{1}{p^{r-1}(p-1)}$. *Then* $E_p(\gamma)$ *is a primitive* $(p^r)^{th}$ *root of unity.*

Before we begin with the proof of the theorem, we first observe the $p$-adic analytic properties of the power series, $S(t)$. It can be seen that $S(t)$ converges on the open unit disk, $\{t \in \mathbb{C}_p : \operatorname{ord}_p t > 0\}$ since for $\operatorname{ord}_p t > 0$, $\operatorname{ord}_p\left(\frac{t^{p^j}}{p^j}\right)$ diverges to $\infty$ as $j$ tends to $\infty$. Also from the theory of Newton polygons and the *p-adic Weierstrass Preparation Theorem* ([Kob84]), it can be shown that for every positive integer $r$, there exist $p^{r-1}(p-1)$ zeros, $\gamma_{i,r}$ of $S(t)$ each of which satisfying $\operatorname{ord}_p \gamma_{i,r} = \dfrac{1}{p^{r-1}(p-1)}$, for $i = 1, 2, ..., p^{r-1}(p-1)$. Since, we will need this result in the later sections, we will state

this as a proposition.

**Proposition 2.1.2.** *Let* $S(t) := \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$. *Let* $r$ *be a positive integer. Then there exist* $p^{r-1}(p-1)$ *zeros,* $\gamma_{i,r}$ *of* $S(t)$ *each of which satisfying* $\operatorname{ord}_p \gamma_{i,r} = \dfrac{1}{p^{r-1}(p-1)}$, *for* $i = 1, 2, ..., p^{r-1}(p-1)$.

*Proof.* We first write $S(t)$ as

$$\begin{aligned} S(t) &= \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j} \\ &= t + \frac{t^p}{p} + \frac{t^{p^2}}{p^2} + \frac{t^{p^3}}{p^3} + ... \\ &= t\left(1 + \frac{t^{p-1}}{p} + \frac{t^{p^2-1}}{p^2} + ...\right) \\ &= t\tilde{S}(t) \end{aligned}$$

where $\tilde{S}(t) = 1 + \sum_{j=1}^{\infty} \frac{t^{(p^j-1)}}{p^j}$. Then, the Newton Polygon of $\tilde{S}(t)$ is well defined ([Kob84]). The Newton Polygon is the convex closure of the points $(p^j - 1, \operatorname{ord}_p p^{-j}) = (p^j - 1, -j)$ along with the origin. Then by the Corollory to Theorem 14 (*The p-adic Weierstrass Preparation Theorem*) ([Kob84], Chapter IV), it follows that for each $r \geq 1$, $\tilde{S}(t)$ (and hence $S(t)$) has $p^r - p^{r-1} = p^{r-1}(p-1)$ zeros $\gamma_{i,r}$ satisfying $\operatorname{ord}_p \gamma_{i,r} = \frac{1}{p^{r-1}(p-1)}$, for $i = 1, 2, ..., p^{r-1}(p-1)$. □

In order to prove the theorem, we need the following lemma.

**Lemma 2.1.3.** *Let* $S(t) := \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$. *Let* $r$ *be a positive integer. If* $\operatorname{ord}_p(t) > \dfrac{1}{p^{r-1}(p-1)}$, *then* $\operatorname{ord}_p\left(p^{r-1}S(t)\right) > \dfrac{1}{p-1}$ *and the power series,* $\exp_p(p^{r-1}S(t)) = \sum_{i=0}^{\infty} \frac{\left(p^{r-1}S(t)\right)^i}{i!}$ *converges p-adically and* $E_p(t)^{p^{r-1}} = \exp_p(p^{r-1}S(t))$ *for* $\operatorname{ord}_p(t) > \dfrac{1}{p^{r-1}(p-1)}$.

*Proof.* We first note that the series $\exp_p(u) = \sum_{j=0}^{\infty} \frac{u^j}{j!}$ converges $p$-adically only[1] for $\operatorname{ord}_p u > \frac{1}{p-1}$. But since $E_p(u) \in \mathbb{Z}_p[[u]]$, it converges for $\operatorname{ord}_p u > 0$. And the series

[1]Please note that the convergence of a $p$-adic power series only depends on the $p$-adic size (absolute value) of its coefficients and hence there is no notion of conditional convergence.

$E_p(t)^{p^{r-1}}$ equals the series $\exp_p(p^{r-1}S(t))$ as a formal power series. Hence, it suffices to prove the first part of the lemma and the second part follows automatically.

Now let $c = \mathrm{ord}_p(t) > \dfrac{1}{p^{r-1}(p-1)}$. Then

$$\begin{aligned}\mathrm{ord}_p\left(p^{r-1}S(t)\right) &= \mathrm{ord}_p\left(\sum_{j=0}^{\infty}\frac{t^{p^j}}{p^{j-(r-1)}}\right)\\ &\geq \inf_{j\geq 0}\left(p^j c - j + (r-1)\right).\end{aligned}$$

We now observe that $p^j c - j + (r-1)$ is strictly increasing for $j \geq r$. For $j \geq r$, we have that $p^{j+1}c - (j+1) + (r-1) > p^j c - j + (r-1)$ if and only if $p^{j+1}c - p^j c > 1$. And indeed,

$$\begin{aligned}p^{j+1}c - p^j c &= p^j c(p-1)\\ &\geq p^r c(p-1)\\ &> p^r\left(\frac{1}{p^{r-1}(p-1)}\right)(p-1)\\ &= p > 1.\end{aligned}$$

Hence,

$$\begin{aligned}\mathrm{ord}_p\left(p^{r-1}S(t)\right) &\geq \inf_{j\geq 0}\left(p^j c - j + (r-1)\right)\\ &= \min_{0\leq j\leq r}\left(p^j c - j + (r-1)\right).\end{aligned}$$

It can easily be verified that $p^j c - j + (r-1) > \frac{1}{p-1}$ for all $0 \leq j \leq r$ as follows. When $j = r$, we have

$$p^j c = p^r c > \frac{p^r}{p^{r-1}(p-1)} = \frac{p}{p-1} = 1 + \frac{1}{p-1}.$$

Hence, $p^j c - j + (r-1) > \frac{1}{p-1}$ in this case. When $j = r-1$, we have

$$p^j c = p^{r-1}c > \frac{p^{r-1}}{p^{r-1}(p-1)} = \frac{1}{p-1}.$$

Hence, $p^j c - j + (r-1) > \frac{1}{p-1}$ in this case as well. Finally when $0 \leq j \leq (r-2)$, we

have

$$p^j c - j + (r-1) \geq p^j c + 1 > \frac{p^j}{p^{r-1}(p-1)} + 1 > 1 \geq \frac{1}{p-1}.$$

Thus,

$$\operatorname{ord}_p \left(p^{r-1} S(t)\right) = \min_{0 \leq j \leq r} \left(p^j c - j + (r-1)\right) > \frac{1}{p-1}$$

and the lemma is proved. □

We can now prove Theorem 2.1.1.

*Proof of Theorem 2.1.1.* Suppose $\gamma$ is a zero of $S(t)$ satisfying $\operatorname{ord}_p \gamma = \dfrac{1}{p^{r-1}(p-1)}$ for some positive integer $r$. We may write $E_p(t) = 1 + \sum_{j=1}^{\infty} b_j t^j$ for some coefficients $b_j$ satisfying $\operatorname{ord}_p b_j \geq 0$ using Dwork's Lemma ([Kob84]). Then $E_p(\gamma) = 1 + \alpha$, where $\alpha = \sum_{j=1}^{\infty} b_j \gamma^j$ with

$$\begin{aligned} \operatorname{ord}_p \alpha &= \operatorname{ord}_p \left(b_1\gamma + b_2\gamma^2 + ...\right) \\ &\geq \min_{j \geq 1} \left[\operatorname{ord}_p b_j + \frac{j}{p^{r-1}(p-1)}\right] \\ &\geq \frac{1}{p^{r-1}(p-1)}. \end{aligned}$$

But for $j \geq 2$,

$$\operatorname{ord}_p(b_j \gamma^j) \geq \frac{2}{p^{r-1}(p-1)} > \frac{1}{p^{r-1}(p-1)}.$$

Also noting that $b_1$ is in fact equal to 1 (by expanding the Artin-Hasse exponential series, $E_p(t)$ as an infinite product of infinite series and computing the coefficient of $t$), we have that $\operatorname{ord}_p(b_1\gamma) = \frac{1}{p^{r-1}(p-1)}$. Then by the property of the non-Archimedian metric, we have that

$$\operatorname{ord}_p \alpha = \frac{1}{p^{r-1}(p-1)}.$$

In particular, this implies that $\alpha \neq 0$ and hence, $E_p(\gamma) \neq 1$. On the other hand, since

$\operatorname{ord}_p \gamma = \frac{1}{p^{r-1}(p-1)} > \frac{1}{p^r(p-1)}$, by the lemma above, we may write

$$E_p(\gamma)^{p^r} = \exp\left[p^r S(\gamma)\right] = \exp(0) = 1.$$

Hence, $E_p(\gamma)$ is indeed a $p$-adic $p^r$-th root of unity. Lastly, we need to show that $E_p(\gamma)$ is a *primitive* $p^r$-th root of unity. When $r = 1$, this is clear. When $r \geq 2$, $E_p(\gamma) = 1 + \alpha$ satisfies the equation $x^{p^r} - 1 = 0$. Writing $x^{p^r} - 1 = (x^{p^{r-1}} - 1)\Phi_{p^r}(x)$, where $\Phi_{p^r}(x)$ is the $p^r$-th cyclotomic polynomial, we must have that if $1 + \alpha$ is *not a primitive* $p^r$-th root of unity, then it must satisfy the equation $x^{p^{r-1}} - 1 = 0$. But then $1 + \alpha$ and hence $\alpha$ must belong to the field $\mathbb{Q}_p(\zeta_{p^{r-1}})$, where $\zeta_{p^{r-1}}$ is a $p$-adic primitive $p^{r-1}$-th root of unity. Also the field extension $\mathbb{Q}_p(\zeta_{p^{r-1}})$ is *totally ramified* over $\mathbb{Q}_p$ ([Kob84]: Chapter III, Section 3) with ramification index, $e = p^{r-2}(p-1)$. But then since $\alpha \in \mathbb{Q}_p(\zeta_{p^{r-1}})$ and $\operatorname{ord}_p \alpha > 0$, we must have that $\operatorname{ord}_p \alpha \geq \frac{1}{e} = \frac{1}{p^{r-2}(p-1)}$, contradicting the fact that $\operatorname{ord}_p \alpha = \frac{1}{p^{r-1}(p-1)}$. □

We are now ready to construct Dwork's splitting functions.

Let $r$ be a positive integer. For each $i = 1, 2, ..., r$, let $\gamma_i$ be a zero of $S(t) = \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$ satisfying $\operatorname{ord}_p \gamma_i = \frac{1}{p^{i-1}(p-1)}$. Then we define the function $\theta_{\gamma_i}(t)$ associated with $\gamma_i$ to be

$$\theta_{\gamma_i}(t) := E_p(\gamma_i t) = \exp\left(\sum_{j=0}^{\infty} \frac{(\gamma_i t)^{p^j}}{p^j}\right).$$

We almost always abbreviate and write $\theta_i(t)$ to denote $\theta_{\gamma_i}(t)$ and assume that $\gamma_i$ has already been chosen. It can be shown that the function $\boxed{\hat{\theta}_r(t) := \prod_{i=1}^{r} \theta_i(t)}$ is a *splitting function at level* $r$ in the sense of Dwork and Blache [Bla03] when the $\gamma_i$ are chosen consistently. We will soon explain how to choose a collection $\{\gamma_i : i = 1, 2, ..., r\}$ consistently, in an obvious fashion.

**Proposition 2.1.4.** *With the above notation, each function $\theta_i(t)$ has its $p$-adic radius of convergence equal to $p^{\left(\frac{1}{p^{i-1}(p-1)}\right)}$. In particular, $\theta_i(t)$ converges for $\operatorname{ord}_p t > -\frac{1}{p^{i-1}(p-1)}$.*

*Proof.* The proof is a trivial consequence of the facts that $E_p(t) \in \mathbb{Z}_p[[t]]$ and $\operatorname{ord}_p \gamma_i =$

$\frac{1}{p^{i-1}(p-1)}$. Writing $E_p(t) = \sum_{j=0}^{\infty} B_j t^j$ for some $B_j$ satisfying $\operatorname{ord}_p B_j \geq 0$, we have that $\theta_i(t) = \sum_{j=0}^{\infty} B_j \gamma_i^j t^j$ and $\operatorname{ord}_p \left( B_j \gamma_i^j t^j \right) \geq \frac{j}{p^{i-1}(p-1)} + j \operatorname{ord}_p t$ where the right hand side tends to $+\infty$ as $j$ tends to $+\infty$ whenever $\operatorname{ord}_p t > -\frac{1}{p^{i-1}(p-1)}$. Hence, $\theta_i(t)$ converges for $\operatorname{ord}_p t > -\frac{1}{p^{i-1}(p-1)}$. On the other hand, it can be shown that $E_p(t)$ has its $p$-adic radius of convergence exactly equal to 1 (please see lemma below), from which it follows that $\theta_r(t)$ has its $p$-adic radius of convergence exactly equal to $p^{\left(\frac{1}{p^{i-1}(p-1)}\right)}$. □

**Lemma 2.1.5.** *The series $E_p(t)$ does not converge for $\operatorname{ord}_p t = 0$ and has its $p$-adic radius of convergence exactly equal to 1.*

*Proof.* Since $E_p(t) \in \mathbb{Z}_p[[t]]$, it converges for $\operatorname{ord}_p t > 0$. Thus we only need to show that $E_p(t)$ does not converge for $\operatorname{ord}_p t = 0$. For a non-zero real number $b$, let $D(b)$ denote the *closed disk* of radius $b$, that is, $D(b) = \{x \in \mathbb{C}_p : |x|_p \leq b\}$.

We first observe that for any power series, $f(t) = \sum_{i=0}^{\infty} a_i t^i \in \mathbb{Z}_p[[t]]$, if $f(t)$ converges in the closed disk, $D(1)$ and if at least *two* of the coefficients $a_i$ are not divisible by $p$, then $f(t)$ has a zero in $D(1)$. This is because the Newton polygon of the modified power series $f_1(t) = \dfrac{f(t)}{a_n t^n}$ (where $a_n$ is the first non-zero coefficient of $f(t)$) has at least one edge with a non-positive slope. And by the *Weierstrass' Preparation Theorem* ([Kob84]), $f_1(t)$ and hence $f(t)$ has at least one zero in $D(1)$.

We also observe another fact as a consequence of the *Weierstrass' Preparation Theorem* ([Kob84]). If a power series, $f(t) = \sum_{i=0}^{\infty} a_i t^i \in \mathbb{C}_p[[t]]$ convergent on $D(b)$ for some $b > 0$ has infinitely many zeros in $D(b)$, then $f(t) \equiv 0$.

Now suppose $E_p(t)$ converges for $\operatorname{ord}_p t = 0$. Then, it converges on $D(1)$ and by the first observation, there exists some $\alpha \in D(1)$ such that $E_p(\alpha) = 0$. Let $\beta$ be a $p$-th root of $\alpha$. Then $\operatorname{ord}_p \beta = \left(\dfrac{1}{p}\right) \operatorname{ord}_p \alpha \geq 0$. So $E_p(\beta)$ converges. And since $E_p(t^p) \exp(pt) = E_p(t)^p$ as formal power series and since $E_p(\beta^p) = 0$, it follows that $E_p(\beta) = 0$ as well. In this way we can construct an *infinite* sequence of zeros of $E_p(t)$ in the disk $D(1)$.

(If $\beta$ is a Teichmuller unit, we can fix a primitive $p$-th root of 1 say $\zeta_p$ and produce the sequence $(\zeta_p \beta)^{p^\ell}$ instead. But $(\zeta_p \beta)^{p^\ell} \neq \zeta_p \beta$ for any $\ell$. So we produce in this case

as well a sequence of distinct zeros of $E_p(t)$ in the disk $D(1)$.)

Then by the second observation, $E_p(t) \equiv 0$, which is a contradiction. $\square$

### 2.1.2 Construction of Characters from Splitting Functions

Let $r$ be a fixed positive integer. Let $\{\gamma_1, \gamma_2, ..., \gamma_r\}$ be a consistent family of zeros of $S(t) = \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$ in the sense that $E_p(\gamma_r) = \theta_r(1)$ is a primitive $p^r$-th root of unity and $E_p(\gamma_{r-i}) = E_p(\gamma_r)^{p^i}$ for $i = 1, 2, ..., r-1$. Let $\zeta_{p^r} = \theta_r(1)$. We define the character $\boxed{\Theta^{(r)} : \mathbb{Z}_p/p^r\mathbb{Z}_p \to \mathbb{C}_p}$ by $\Theta^{(r)}(\bar{x}) := \theta_r(1)^x$ where $x \in \mathbb{Z}_p$ is any lift of $\bar{x} \in \mathbb{Z}_p/p^r\mathbb{Z}_p$ satisfying $x \equiv \bar{x} \pmod{p^r\mathbb{Z}_p}$.

We first note that for $w \in \mathbb{Z}_p$ being any lift of $\bar{x} \in \mathbb{Z}_p/p^r\mathbb{Z}_p$ satisfying $w \equiv \bar{x} \pmod{p^r\mathbb{Z}_p}$, the power series $\theta_r(1)^w$ is evaluated as the binomial expansion

$$(1+y)^w = \sum_{j=0}^{\infty} \binom{w}{j} y^j$$

where $y = \theta_r(1) - 1 = E_p(\gamma_r) - 1 = \zeta_{p^r} - 1$. We represent the series $(1+y)^w$ by $B_{w,p}(y)$ and since $w \in \mathbb{Z}_p$, $B_{w,p}(y) \in \mathbb{Z}_p[[y]]$ (please see [Kob84]: Chapter IV) and thus the series converges when $\mathrm{ord}_p\, y > 0$. Indeed $\mathrm{ord}_p\, y = \mathrm{ord}_p(\zeta_{p^r} - 1) = \dfrac{1}{p^{r-1}(p-1)} > 0$ as $y$ being a root of the Eisenstein polynomial,

$$g_{p^r}(z) := \Phi_{p^r}(z+1) = (z+1)^{p^{r-1}(p-1)} + (z+1)^{p^{r-1}(p-2)} + ... + (z+1)^{p^{r-1}} + 1$$

is a generator of the *totally ramified* extension $\mathbb{Q}_p(\zeta_{p^r})$ of degree $p^{r-1}(p-1)$ over $\mathbb{Q}_p$.

We also note that this definition of the character is independent of the choice of $x$ by Theorem 2.1.1. And in particular, we understand that $\theta_r(1)^x$ degenerates to 1 when $x \equiv 0 \pmod{p^r\mathbb{Z}_p}$. Although *any* lift $x \in \mathbb{Z}_p$ of $\bar{x} \in \mathbb{Z}_p/p^r\mathbb{Z}_p$ can be used to evaluate the character values, certain special lifts called as the *Teichmüller lifts* have some *good* properties in the sense that the series $\theta_r(1)^x$ can be evaluated in a much simpler way rather than using the original binomial expansion. Before we discuss the use of the *Teichmüller lifts*, we make the following remark about our generalization of

Dwork's original splitting function which he used in the proof of the rationality of the zeta function.

**Remark 2.1.6.** Dwork's original splitting function corresponds to the case when $r = 1$. We will refer to this special case whenever we want to emphasize certain key ideas used in the development of Dwork's Trace Formula.

---

We will now provide a very brief review of the theory of unramified extensions and Teichmüller lifts. We will omit proofs, and include a few in the Appendix B.

---

**Proposition 2.1.7.** *Let $f$ be a positive integer. There exists a unique unramified extension, $K_f^{\text{unram}}$ of $\mathbb{Q}_p$ of degree $f$ and it can be obtained by adjoining a primitive $(p^f-1)$-th root of 1. If $K$ is an extension of $\mathbb{Q}_p$ of degree $n$, index of ramification $e$ and residue field degree $f$ (so that $n = ef$), then $K = K_f^{\text{unram}}(\pi)$ where $\pi$ satisfies an Eisenstein polynomial of degree $e$ with coefficients in $K_f^{\text{unram}}$.*

*Proof.* Please see [Kob84]: Chapter III, Section 3. □

We will denote by $\mathbb{Q}_{p^f}$ the unique unramified extension of degree $f$ over $\mathbb{Q}_p$ and by $\mathbb{Z}_{p^f}$, the ring of integers of $\mathbb{Q}_{p^f}$. Then we have the following results as stated in Chapter III of [Kob84] and Appendix B of [Mus11].

**Proposition 2.1.8.** *Let $f$ be a positive integer. Then for every $\alpha \in \mathbb{F}_{p^f}$, there exists a unique $\tilde{\alpha} \in \mathbb{Z}_{p^f}$ such that*

*(i) $\tilde{\alpha}$ is a lift of $\alpha$, that is, $\tilde{\alpha} \equiv \alpha \pmod{p\mathbb{Z}_{p^f}}$. In other words, the image of $\tilde{\alpha}$ in the quotient $\mathbb{Z}_{p^f}/p\mathbb{Z}_{p^f}$ corrsponds to $\alpha$ under the isomorphism of the residue field, $\mathbb{Z}_{p^f}/p\mathbb{Z}_{p^f} \cong \mathbb{F}_{p^f}$.*

*(ii) $\tilde{\alpha}^{p^f} = \tilde{\alpha}$, that is, $\tilde{\alpha}$ is either 0 or a $(p^f-1)$-th root of unity.*

*Proof.* Please see Appendix B. □

**Definition 2.1.9.** The $\tilde{\alpha}$ corresponding to $\alpha$ as stated in the above proposition is called the *Teichmüller lift* of $\alpha$ in the unramified extension $\mathbb{Q}_{p^f}$. And we often call the *nonzero* Teichmüller lifts as *Teichmüller units*, justified by the fact that they are roots of unity.

**Corollary 2.1.10.** *Every element $\alpha \in \mathbb{Z}_{p^f}$ has a unique expression as the sum of a series $\sum_{i\geq 0} a_i p^i$, where $a_i^{p^f} = a_i$ for every $i$.*

*More generally, if $K$ is a finite extension of $\mathbb{Q}_p$ of degree $n$, index of ramification $e$, and residue field degree $f$, and if $\pi$ is chosen so that $\operatorname{ord}_p \pi = 1/e$, then every $\alpha \in K$ can be written uniquely as*

$$\sum_{i=m}^{\infty} a_i \pi^i$$

*where $m = e \operatorname{ord}_p \alpha$ and each $a_i$ satisfies $a_i^{p^f} = a_i$ (the $a_i$ are called the Teichmüller digits).*

*Proof.* Please see Appendix B. □

Having stated the basic properties of Teichmüller units, we will state two more propositions which describe the Galois group of $\mathbb{Q}_{p^f}$ over $\mathbb{Q}_p$ and the behaviour of the Teichmüller units under the action of this Galois group.

**Proposition 2.1.11.** *Let $f$ be a positive integer. Then $\mathbb{Q}_{p^f}$ is a Galois extension of $\mathbb{Q}_p$ and there is an isomorphism of Galois groups $Gal(\mathbb{Q}_{p^f}/\mathbb{Q}_p) \cong Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$ that associates to each automorphism of $\mathbb{Q}_{p^f}$, the induced automorphism of the residue field.*

*Proof.* Please see Appendix B. □

The isomorphism in the above proposition allows us to talk about the *Frobenius generator* of $Gal(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$ which is the element corresponding to the Frobenius generator of $Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$. We end our brief review of the theory of unramified extensions and Teichmüller lifts with the following trivial lemma.

**Lemma 2.1.12.** *Let $\overline{\sigma}$ be the Frobenius generator of $Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$ and let $\sigma$ be the corresponding Frobenius generator of $Gal(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$ under the isomorphism in Proposition 2.1.11. Then for $x \in \mathbb{Z}_{p^f}$ satisfying $x \equiv \bar{x} \pmod{p\mathbb{Z}_{p^f}}$, we have*

*(i)* $\sigma(x) \equiv x^p \pmod{p\mathbb{Z}_{p^f}}$

*(ii) If moreover $x$ is a Teichmüller lift of $\bar{x}$, i.e., if $x$ satisfies $x^{p^f} = x$, then $\sigma(x) = x^p$ and $\sigma(x)$ is also a Teichmüller lift.*

*Proof.* Please see Appendix B. □

---

We now state an important application of the Teichmüller lifts.

**Proposition 2.1.13.** *For the case when $r = 1$, if $x \in \mathbb{Z}_p$ is a Teichmüller lift of $\bar{x} \in \mathbb{F}_p$, then $\Theta^{(1)}(\bar{x}) := \theta_1(1)^x = \theta_1(x)$.*

Before we present the proof, we observe that the Teichmüller lifts enable us in evaluating the values of the character $\Theta^{(r)}(\bar{x})$ by realizing it as a more tangible $p$-adic analytic expression. The proof can easily be generalized to obtain a similar expression in terms of Teichmüller lifts for $\Theta^{(r)}(\bar{x})$ when $r > 1$. We will present the proof of the base case when $r = 1$ to emphasize the key ideas.

*Proof.* The case when $x$ is 0 is trivial. So we consider $x \neq 0$ (and hence $\bar{x} \neq 0$). We first observe that from the proof of Proposition 2.1.4, we may write the power series $\theta_1(t)$ as

$$\begin{aligned}\theta_1(t) &= 1 + \sum_{j=1}^{\infty} b_j t^j \\ &= 1 + b(t)\end{aligned}$$

for some coefficients $b_j$ satisfying $\operatorname{ord}_p b_j \geq \dfrac{j}{p-1}$, and thus $b(t) := \sum\limits_{j=1}^{\infty} b_j t^j$ satisfies $\operatorname{ord}_p b(t) \geq \dfrac{1}{p-1}$ whenever $\operatorname{ord}_p t \geq 0$.

We now consider the two formal power series $f(y) := \theta_1(y)^x$ and $g(y) := \theta_1(yx)$. We will show that both these series converge for $\mathrm{ord}_p\, y \geq 0$ and that they are equal in a small disk about the origin, $y = 0$, and hence deduce that $f(y) = g(y)$ on the whole disk $\mathrm{ord}_p\, y \geq 0$ and in particular $f(1) = g(1)$ which proves the proposition.

Now, since $x$ is a unit, $\mathrm{ord}_p\, x = 0$ and hence the series, $f(y) = [1+b(y)]^x = B_x(b(y))$ converges for $\mathrm{ord}_p\, b(y) > 0$ ([Kob84]: Chapter IV). Thus by the first observation $f(y)$ converges for $\mathrm{ord}_p\, y \geq 0$. On the other hand, $g(y) = \theta_1(yx) = 1 + \sum_{j=0}^{\infty} b_j x^j y^j$, and since $\mathrm{ord}_p\, x = 0$, $\mathrm{ord}_p(b_j x^j) = \mathrm{ord}_p\, b_j \geq \dfrac{j}{p-1}$. Then by Proposition 2.1.4, $g(y)$ converges for $\mathrm{ord}_p\, y > -\dfrac{1}{p-1}$. In particular we have that both $f(y)$ and $g(y)$ converge on the disk $\mathrm{ord}_p\, y \geq 0$.

Next, we observe that when $y \to 0$, both $f(y)$ and $g(y)$ converge to 1 since they are continuous at the origin. Now since the $p$-adic logarithm function $\log_p(1+z)$ converges for $\mathrm{ord}_p > 0$, we see that when $\mathrm{ord}_p\, y >> 0$, then $f(y)$ and $g(y)$ are sufficiently close to 1 and $\log_p f(y)$ and $\log_p g(y)$ are defined and we have that

$$f(y) = g(y) \iff \log_p f(y) = \log_p g(y)$$

because of the local invertibility of the $p$-adic logarithm function [Kob84].

Hence we are left to show that $\log_p f(y) = \log_p g(y)$ on a small disk about the origin $y = 0$, that is, when $\mathrm{ord}_p\, y$ is sufficiently large. This follows from simple algebra along with using the hypothesis that $x$ is a Teichmüller lift at a crucial step. We have

$$\begin{aligned}
\log_p g(y) &= \log_p \theta_1(yx) \\
&= \log_p \left[ \exp_p \left( \sum_{j=0}^{\infty} \frac{(\gamma_1 yx)^{p^j}}{p^j} \right) \right] \\
&= \sum_{j=0}^{\infty} \frac{(\gamma_1 yx)^{p^j}}{p^j} \\
&= x \sum_{j=0}^{\infty} \frac{(\gamma_1 y)^{p^j}}{p^j}
\end{aligned}$$

$$
\begin{aligned}
&= x \log_p \left[ \exp_p \left( \sum_{j=0}^{\infty} \frac{(\gamma_1 y)^{p^j}}{p^j} \right) \right] \\
&= x \log_p \theta_1(y) \\
&= \log_p \theta_1(y)^x \\
&= \log_p f(y)
\end{aligned}
$$

where the third and the fifth equalities follow from the local invertibility of the $p$-adic logarithm function, the fourth equality follows from the fact that $x$ is a Teichmüller lift and the penultimate equality follows from the equality of the formal power series $\log_p(1+z)^w$ and $w \log_p(1+z)$ in the ring $\mathbb{Q}[w][[z]]$ with their coefficients being polynomials in $w$, and hence when $w \in \mathbb{Q}_p$ and when $\mathrm{ord}_p\, z >> 0$, both the power series converge and are equal. Hence, we have the proposition. □

Having proven this proposition, we can now readily generalize this using the same methods to obtain the following results.

**Proposition 2.1.14.** *If $x \in \mathbb{Z}_q$ satisfies $x^q = x$, then*

$$\theta_1(1)^{x+x^p+x^{p^2}+\ldots+x^{p^{a-1}}} = \theta_1(x)\theta_1(x^p)\theta_1(x^{p^2})\ldots\theta_1(x^{p^{a-1}})$$

*and more generally, for each $j = 1, 2, 3, ..., r$, we have*

$$\theta_j(1)^{x+x^p+x^{p^2}+\ldots+x^{p^{a-1}}} = \theta_j(x)\theta_j(x^p)\theta_j(x^{p^2})\ldots\theta_j(x^{p^{a-1}})$$

*that is,*

$$\theta_j(1)^{\sum_{i=0}^{a-1} x^{p^i}} = \prod_{i=0}^{a-1} \theta_j(x^{p^i})$$

*or in other words,*

$$\theta_j(1)^{\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x)} = \prod_{i=0}^{a-1} \theta_j(\sigma^i(x))$$

*where $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}$ is the trace map and $\sigma$ is the Frobenius generator of $Gal(\mathbb{Q}_q/\mathbb{Q}_p)$.*

*Proof.* We imitate the same method of proof of the previous proposition. Let us fix $j \in \{1, 2, ..., r\}$. Again, the case when $x = 0$ is trivial and we assume $x \neq 0$. Consider

the two formal power series, $f_j(y) := \theta_j(y)^{\sum_{i=0}^{a-1} x^{p^i}}$ and $g_j(y) := \prod_{i=0}^{a-1} \theta_j(yx^{p^i})$ in $\mathbb{C}_p[[y]]$. We will show that both these series converge for $\mathrm{ord}_p\, y \geq 0$ and that they are equal in a small disk about the origin, $y = 0$, and hence deduce that $f(y) = g(y)$ on the whole disk $\mathrm{ord}_p\, y \geq 0$ and in particular $f(1) = g(1)$ which proves the proposition.

From the proof of Proposition 2.1.4, we observe that we may write the power series $\theta_j(t)$ as

$$\begin{aligned}\theta_j(t) &= 1 + \sum_{i=1}^{\infty} b_i t^i \\ &= 1 + b(t)\end{aligned}$$

for some coefficients $b_i$ satisfying $\mathrm{ord}_p\, b_i \geq \dfrac{i}{p^{j-1}(p-1)}$, and thus $b(t) := \sum_{i=1}^{\infty} b_i t^i$ satisfies $\mathrm{ord}_p\, b(t) \geq \dfrac{1}{p^{j-1}(p-1)}$ whenever $\mathrm{ord}_p\, t \geq 0$.

Then on one hand, since $\sum_{i=0}^{a-1} x^{p^i} = \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x) \in \mathbb{Z}_p$, $f_j(y) = \theta_j(y)^{\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x)} = [1+b(y)]^{\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x)}$ converges whenever $\mathrm{ord}_p\, b(y) > 0$ ([Kob84]: Chapter IV). And hence, by the previous paragraph, $f_j(y)$ converges for $\mathrm{ord}_p\, y \geq 0$. On the other hand, any factor $\theta_j(yx^{p^k})$ of $g_j(y)$, for $k \in \{0, 1, ...a-1\}$ can be written as

$$\theta_j(yx^{p^k}) = 1 + \sum_i b_i y^i x^{ip^k}$$

and since $x$ is a unit, $\mathrm{ord}_p\, b_i x^{ip^k} = \mathrm{ord}_p\, b_i \geq \dfrac{i}{p^{j-1}(p-1)}$ from the observation in the previous paragraph. Hence, the factor $\theta_j(yx^{p^k})$ converges whenever $\mathrm{ord}_p\, y > -\dfrac{1}{p^{j-1}(p-1)}$. Hence, in particular, $g_j(y)$ being a finite product of these factors converges for $\mathrm{ord}_p\, y \geq 0$.

Again we may imitate the argument in the proof of the previous proposition by observing that both $f_j(y)$ and $g_j(y)$ converge to 1 as $y$ tends to 0 since thy are both continuous at the origin. Then on a very small disk about the origin, that is, when $\mathrm{ord}_p\, y > M$ for some sufficiently large $M > 0$, $\log_p f_j(y)$ and $\log_p g_j(y)$ are defined, and thus it suffices to show that $\log_p f_j(y) = \log_p g_j(y)$ by the local invertibility of the $p$-adic logarithm function.

Now,

$$\begin{aligned}
\log_p g_j(y) &= \sum_{k=0}^{a-1} \log_p \theta_j(yx^{p^k}) \\
&= \sum_{k=0}^{a-1} \log_p \left[ \exp_p \left( \sum_{l=0}^{\infty} \frac{[\gamma_j y x^{p^k}]^{p^l}}{p^l} \right) \right] \\
&= \sum_{k=0}^{a-1} \sum_{l=0}^{\infty} \frac{[\gamma_j y x^{p^k}]^{p^l}}{p^l} \\
&= \sum_{l=0}^{\infty} \frac{[\gamma_j y]^{p^l}}{p^l} \sum_{k=0}^{a-1} x^{p^{l+k}} \\
&= \sum_{l=0}^{\infty} \frac{[\gamma_j y]^{p^l}}{p^l} \sum_{k=0}^{a-1} x^{p^k} \\
&= \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x) \sum_{l=0}^{\infty} \frac{[\gamma_j y]^{p^l}}{p^l} \\
&= \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x) \log_p \left[ \exp_p \left( \sum_{l=0}^{\infty} \frac{[\gamma_j y]^{p^l}}{p^l} \right) \right] \\
&= \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x) \log_p \left[ \theta_j(y) \right] \\
&= \log_p \left[ \theta_j(y)^{\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x)} \right] \\
&= \log_p f_j(y)
\end{aligned}$$

where we used the hypothesis that $x^q = x$ and the fact that the set $\{l, l+1, ..., l+a-1\}$ is a complete set of residues $\pmod{a}$ for any integer $l$ in the fifth equality above. And the penultimate equality follows from the same argument as we had before in the previous proposition.

Finally, by Lemma 2.1.12, $\sigma(x) = x^p$, and hence it is legitimate to rephrase the conclusion of the theorem as

$$\theta_j(1)^{\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x)} = \prod_{i=0}^{a-1} \theta_j(\sigma^i(x)).$$

□

The proposition above gives a beautiful way of evaluating character values as $p$-adic anaytic expressions. We have the following theorem.

**Theorem 2.1.15.** *If $x \in \mathbb{Z}_q$ is a Teichmüller lift of $\bar{x} \in \mathbb{F}_q$, then*

$$\Theta^{(1)} \circ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\bar{x}) = \theta_1(x)\theta_1(x^p)\theta_1(x^{p^2})...\theta_1(x^{p^{a-1}})$$

*Proof.* Let $\sigma$ be the Frobenius generator of $Gal(\mathbb{Q}_q/\mathbb{Q}_p)$ and $\bar{\sigma}$, the corresponding Frobenius generator of $Gal(\mathbb{F}_q/\mathbb{F}_p)$ as in Proposition 2.1.11. Then we have

$$\begin{aligned}\Theta^{(1)} \circ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\bar{x}) &= \Theta^{(1)}\left(\sum_{i=0}^{a-1} \bar{\sigma}^i(\bar{x})\right) \\ &= \theta_1(1)^{\sum_{i=0}^{a-1}\sigma^i(x)} \\ &= \prod_{i=0}^{a-1} \theta_1(x^{p^i})\end{aligned}$$

where the second equality follows from the fact that $\sum_{i=0}^{a-1} \sigma^i(x)$ lifts $\sum_{i=0}^{a-1} \bar{\sigma}^i(\bar{x})$ and the last equality follows from Proposition 2.1.14. □

Proposition 2.1.14 and Theorem 2.1.15 also motivate us to define and conveniently evaluate characters of $\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$, where $l$ is any positive integer, that are derived from the character $\Theta^{(r)}$ (by composition) by observing that the trace map $\mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}$ induces a map on $\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ into $\mathbb{Z}_p/p^r\mathbb{Z}_p$.

**Proposition 2.1.16.** *For each positive integer $l$ and for each positive integer $m$, the trace map $\mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}$ induces a map, $\boxed{\tau(q,l,m) : \mathbb{Z}_{q^l}/p^m\mathbb{Z}_{q^l} \to \mathbb{Z}_p/p^m\mathbb{Z}_p}$ which is an additive group homomorphism.*

*Proof.* Let $\sigma$ be the Frobenius generator of $Gal(\mathbb{Q}_{q^l}/\mathbb{Q}_p)$. Then for $x \in \mathbb{Z}_{q^l}$, since $\mathrm{ord}_p\, \sigma^i(x) = \mathrm{ord}_p\, x$ for all $i \in \{0, 1, ..., al-1\}$, we have that $\mathrm{ord}_p\, \mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(x) \geq 0$. Thus, $\mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(\mathbb{Z}_{q^l}) \subset \mathbb{Z}_p$. Similarly, $\mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(p^m\mathbb{Z}_{q^l}) \subset p^m\mathbb{Z}_p$ since $\mathrm{ord}_p\, \mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(x) \geq m$ whenever $\mathrm{ord}_p\, x \geq m$. Hence, the map $\tau(q,l,m)$ is well defined. And since $\mathrm{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}$ is $\mathbb{Q}_p$-linear, $\tau(q,l,m)$ is indeed an additive group homomorphism. □

**Remark 2.1.17.** It is easily seen that the trace map $\tau(q,l,m)$ is in fact a $\mathbb{Z}_p/p^r\mathbb{Z}_p$-module homomorphism and is the same as the *generalized trace map*, $\mathrm{Tr}_{GR(p^r,al)/GR(p^r,1)}$

of Galois ring extensions as defined in [Wan03] (Section 14.7). This is by the uniqueness of the group of ring automorphisms of $\mathbb{Z}_{q^l}/p^m\mathbb{Z}_{q^l}$ that fix elements in $\mathbb{Z}_p/p^m\mathbb{Z}_p$. The Frobenius automorphism of $Gal(\mathbb{Q}_{q^l}/\mathbb{Q}_p)$ induces the Frobenius automorphism of $Gal((\mathbb{Z}_{q^l}/p\mathbb{Z}_q)/(\mathbb{Z}_p/p\mathbb{Z}_p))$ which in turn corresponds to the generalized Frobenius automorphism of $Gal((\mathbb{Z}_{q^l}/p^m\mathbb{Z}_{q^l})/(\mathbb{Z}_p/p^m\mathbb{Z}_p))$ as defined in Theorem 14.32 in [Wan03].

We are now in a position to extend the character, $\Theta^{(r)}$ we constructed on $\mathbb{Z}_p/p^r\mathbb{Z}_p$ to a character on $\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ by composing it with the induced map $\tau(q,l,r) : \mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l} \to \mathbb{Z}_p/p^r\mathbb{Z}_p$. We observe that we may write any $\bar{x} \in \mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ as

$$\bar{x} = \sum_{i=0}^{r-1} a_i p^i$$

where the $a_i$ are Teichmüller digits satisfying $a_i^{q^l} = a_i$ as in Corollory 2.1.10. Then Theorem 2.1.15 extends to the following theorem.

**Theorem 2.1.18** (Dwork-Blache [Bla03])**.** *Given $\bar{x} \in \mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$, writing $\bar{x} = \sum_{j=0}^{r-1} a_j p^j$ in terms of Teichmüller digits $a_j$ satisfying $a_j^{q^l} = a_j$, we have*

$$\Theta^{(r)} \circ \tau(q,l,r)(\bar{x}) = \prod_{j=0}^{r-1} \prod_{i=0}^{al-1} \theta_{r-j}(a_j^{p^i})$$

*Proof.* Let $\sigma$ be the Frobenius generator of $Gal(\mathbb{Q}_q/\mathbb{Q}_p)$. Then we have,

$$\begin{aligned}
\Theta^{(r)} \circ \tau(q,l,r)(\bar{x}) &= \Theta^{(r)} \left( \sum_{i=0}^{a-1} \sigma^i \left( \sum_{j=0}^{r-1} a_j p^j \right) \right) \\
&= \Theta^{(r)} \left( \sum_{i=0}^{a-1} \sum_{j=0}^{r-1} p^j \sigma^i(a_j) \right) \\
&= \Theta^{(r)} \left( \sum_{j=0}^{r-1} p^j \sum_{i=0}^{a-1} \sigma^i(a_j) \right) \\
&= \Theta^{(r)} \left( \sum_{j=0}^{r-1} p^j \operatorname{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(a_j) \right) \\
&= \prod_{j=0}^{r-1} \Theta^{(r)} \left( p^j \operatorname{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(a_j) \right)
\end{aligned}$$

$$= \prod_{j=0}^{r-1} \theta_r(1)^{p^j \operatorname{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(a_j)}$$
$$= \prod_{j=0}^{r-1} \theta_{r-j}(1)^{\operatorname{Tr}_{\mathbb{Q}_{q^l}/\mathbb{Q}_p}(a_j)}$$
$$= \prod_{j=0}^{r-1} \prod_{i=0}^{al-1} \theta_{r-j}(a_j^{p^i})$$

where the second equality is due to the fact that $\sigma$ fixes $\mathbb{Q}_p$, the fifth equality is because $\Theta^{(r)}$ is an additive character and the seventh equality is due to our choice of the consistent family $\{\gamma_1, \gamma_2, ..., \gamma_r\}$ of zeros of $S(t) = \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$ so that $\theta_{r-i}(1) = E_p(\gamma_{r-i}) = E_p(\gamma_r)^{p^i} = \theta_r(1)^{p^i}$ for $i = 1, 2, ..., r-1$; and the last equality follows from the analogue of Proposition 2.1.14 obtained by replacing $q$ with $q^l$. □

### 2.1.3 Sums of Characters constructed from Splitting Functions

The $p$-adic analytic expression obtained for evaluating the values of the characters, $\Theta^{(r)} \circ \tau(q, l, r)$ of $\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ in Theorem 2.1.18 motivates us to obtain an expression for *sums* of these character values associated to an affine algebraic variety defined over $\mathbb{Z}_q/p^r\mathbb{Z}_q$. And then we could study the $L$-functions associated to the family of these character sums and prove *Weil-type* conjectures for these $L$-functions.

Motivated by Proposition 1.5.2, we study the following character sums, that specialize to toric exponential sums over finite fields studied by Dwork in the case when $r = 1$.

**Definition 2.1.19.** Let $\bar{f}(\bar{x}) = \bar{f}(\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) \in (\mathbb{Z}_q/p^r\mathbb{Z}_q)[\bar{x}_1, \bar{x}_2, ..., \bar{x}_n]$ be a polynomial in $n$ variables. Then we define a family, $\{S_l^* : l \geq 1\}$ of exponential sums associated to $\bar{f}(\bar{x})$ as follows:

$$S_l^* = S_l^*(\Theta^{(r)}, \bar{f}) = S_l^*(q, r, \Theta^{(r)}, \bar{f}) := \sum \Theta^{(r)} \circ \tau(q, l, r)(\bar{f}(\bar{x}))$$

where the sum runs over those $\bar{x} = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) \in \left(\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}\right)^n$ with the $\bar{x}_i$ written as $\bar{x}_i = \sum_{k=0}^{r-1} x_{i,k}p^k$ in terms of Teichmüller digits $x_{i,k}$ satisfying $x_{i,k}^{q^l-1} = 1$. It should be noted carefully that the sum is taken over only the Teichmüller *units*, that is, the

$(q^l-1)$-st roots of unity and we discard any $\bar{x}=(\bar{x}_1,\bar{x}_2,...,\bar{x}_n)\in\left(\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}\right)^n$ any of whose components have zero Teichmüller digits.

We also define the $L$-function, $L^*(q,r,\Theta^{(r)},\bar{f},T)$ associated to this family of exponential sums and the polynomial, $\bar{f}(\bar{x})$ by

$$L^*(\Theta^{(r)},\bar{f},T)=L^*(q,r,\Theta^{(r)},\bar{f},T):=\exp\left(\sum_{l=1}^{\infty}\frac{S_l^*T^l}{l}\right)$$

We often abbreviate and denote this $L$-function by $L^*(\bar{f},T)$ for convenience, whenever there is no confusion about the choice of $q,r$ and $\Theta^{(r)}$.

**Remark 2.1.20.** We note that when $r=1$ and when $\bar{f}(\bar{x})$ degenerates to $g_V(x,y)$ as in the discussion following Proposition 1.5.2, then the above family, $\{S_l^*\}$ degenerates to the original family of toric exponential sums considered by Dwork and for which the Dwork trace formula leads to the proof of the rationality of the zeta function of an affine variety through a simple inclusion-exclusion argument ([Bom66], [Dwo60], [AS87a]) which relates $S_l$ as per Definition 1.5.3 and $S_l^*$ as per Definition 2.1.19.

Oue goal now is to obtain an expression for the character sums, $S_l^*$ associated with an arbitrary polynomial, $\bar{f}(\bar{x})=\sum_{\mu}\bar{a}_\mu\bar{x}^\mu$ (where $\bar{a}_\mu\in(\mathbb{Z}_q/p^r\mathbb{Z}_q)$ and $\mu=(\mu_1,\mu_2,...,\mu_n)\in\mathbb{Z}_{\geq 0}^n$ runs over the support of the polynomial, $\bar{f}$, that is, those $\mu$ for which $\bar{a}_\mu\neq 0$, and the notation $\bar{x}^\mu$ means $\prod_{i=1}^{n}\bar{x}_i^{\mu_i}$), using Dwork's $p$-adic theory and prove results for the associated $L$-function.

---

From this point of time until the end of this chapter, we will describe the theory of arriving at a trace formula for the **special case** when $r=1$. In the case when $r=1$, we may identify $(\mathbb{Z}_q/p^r\mathbb{Z}_q)$ with the finite field $\mathbb{F}_q$. In the chapters 3 and 4, we will generalize this theory for any $r\geq 1$.

---

Let $\omega_l : \mathbb{F}_{q^l}^{\times} \to \mathbb{Z}_{q^l}^{\times}$ denote the *Teichmüller character* sending $\bar{y}$ into its unique Teichmüller lift, $y$. Since $\omega_l$ is *multiplicative*, we have the following proposition.

**Proposition 2.1.21.** *Let $\mu = (\mu_1, ..., \mu_n) \in \mathbb{Z}^n$. Let $a_\mu \in \mathbb{Z}_q^{\times}$ and $x_1, x_2, ..., x_n \in \mathbb{Z}_{q^l}^{\times}$ be the Teichmüller lifts of $\bar{a}_\mu \in \mathbb{F}_q$ and $\bar{x}_1, ..., \bar{x}_n \in \mathbb{F}_{q^l}$ respectively. Then the product $a_\mu x^\mu := a_\mu x_1^{\mu_1} ... x_n^{\mu_n}$ is the Teichmüller lift of the product $\bar{a}_\mu \bar{x}^\mu$. Moreover, we have*

$$\begin{aligned}\Theta^{(1)} \circ \tau(q, l, 1)(\bar{a}_\mu \bar{x}^\mu) &= \theta_1(a_\mu x^\mu)\theta_1(a_\mu^p x^{\mu p})...\theta_1(a_\mu^{p^{al-1}} x^{\mu p^{al-1}}) \\ &= \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} \theta_1(a_\mu^{p^j} x^{\mu p^{ia+j}})\end{aligned}$$

*and hence,*

$$\Theta^{(1)} \circ \tau(q, l, 1)(\bar{f}(\bar{x})) = \prod_{\mu \in Supp(\bar{f})} \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} \theta_1(a_\mu^{p^j} x^{\mu p^{ia+j}}) = \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} \prod_{\mu \in Supp(\bar{f})} \theta_1(a_\mu^{p^j} x^{\mu p^{ia+j}})$$

*Proof.* The first assertion follows from the multiplicativity of the Teichmüller character, $\omega_l$ and from the fact that $\omega_l(\bar{a}_\mu) = \omega_1(\bar{a}_\mu) = a_\mu$. The second assertion follows from Theorem 2.1.18 and from the fact that $a_\mu^q = a_\mu$. And the last line follows from the fact that $\Theta^{(1)} \circ \tau(q, l, 1)$ is a character. □

From the above proposition, we can obtain an expression for $\Theta^{(1)} \circ \tau(q, l, 1)(\bar{f}(\bar{x}))$. To do this, we first define a *basic power series associated to* $\bar{f}(\bar{x})$.

**Definition 2.1.22.** We define the power series $F(x) \in \mathbb{Q}_q(\zeta_p)[[x_1, ..., x_n]]$ corresponding to the polynomial $\bar{f}(\bar{x})$ as follows: $F(x) := \prod_{\mu \in Supp(\bar{f})} \theta_1(a_\mu x^\mu)$, where the $a_\mu$ are the Teichmüller lifts of the coefficients $\bar{a}_\mu$.

We then observe that the last expression in the above proposition can be expressed in terms of the action of the Galois group $Gal(\mathbb{Q}_q(\zeta_p)/\mathbb{Q}_p(\zeta_p))$ on the power series $F(x)$. We quickly recall the following porposition.

**Proposition 2.1.23.** *Let $r$ be a positive integer. Then $\mathbb{Q}_q(\zeta_{p^r})$ is Galois over $\mathbb{Q}_p(\zeta_{p^r})$ and*

$$Gal\big(\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})\big) \cong Gal\big(\mathbb{Q}_q/\mathbb{Q}_p\big)$$

*Proof.* Please see Appendix B. □

**Definition 2.1.24.** Let $\sigma$ denote the *Frobenius* generator of $Gal(\mathbb{Q}_q(\zeta_p)/\mathbb{Q}_p(\zeta_p))$. Then for any power series, $H(x) = \sum_{\nu} A(\nu)x^{\nu} \in \mathbb{Q}_q(\zeta_p)[[x_1, x_2..., x_n]]$, we can define the element obtained by the action of $\sigma^i$ on its coefficients as $\boxed{H^{\sigma^i}(x) := \sum_{\nu} \sigma^i(A(\nu))x^{\nu}}$ for $i = 0, 1, 2, ..., (a-1)$.

We can now rewrite the conclusion of Proposition 2.1.21 as follows.

**Proposition 2.1.25.** *Let $l$ be a positive integer and let $x = (x_1, x_2, ..., x_n) \in \left(\mathbb{Z}_{q^l}^{\times}\right)^n$ denote the vector of Teichmüller lifts of the components of the vector $\bar{x} = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) \in \mathbb{F}_{q^l}^n$. Then we have:*

$$\Theta^{(1)} \circ \tau(q, 1, 1)(\bar{f}(\bar{x})) = F(x)F^{\sigma}(x^p)...F^{\sigma^{a-1}}(x^{p^{a-1}}) = \prod_{i=0}^{a-1} F^{\sigma^i}(x^{p^i})$$

*for the case when $l = 1$, and more generally,*

$$\Theta^{(1)} \circ \tau(q, l, 1)(\bar{f}(\bar{x})) = F(x)F^{\sigma}(x^p)...F^{\sigma^{al-1}}(x^{p^{al-1}}) = \prod_{i=0}^{al-1} F^{\sigma^i}(x^{p^i})$$

*which may also be rewritten as*

$$\Theta^{(1)} \circ \tau(q, l, 1)(\bar{f}(\bar{x})) = G_1(x)G_1(x^q)...G_1(x^{q^{l-1}}) = \prod_{i=0}^{l-1} G_1(x^{q^i})$$

*where $G_1(x) = \prod_{i=0}^{a-1} F^{\sigma^i}(x^{p^i})$.*

*(Here, the subscript 1 in $G_1(x)$ refers to the case when $r = 1$. In Chapter 3, we will define an analogous $G_r(x)$ for the general case when $r \geq 1$).*

*Proof.* The proof follows from Proposition 2.1.23, Lemma 2.1.12 and Proposition 2.1.21. And the last equation follows from the fact that the Galois group, $Gal(\mathbb{Q}_q(\zeta_p)/\mathbb{Q}_p(\zeta_p))$ is cyclic of order $a$, that is, $\sigma^a = 1$. We observe that the power series $G_1(x^{q^i})$ converges for $\mathrm{ord}_p\, x_j = 0$ for each $i = 0, 1, ..., l-1$ by the analytical properties of the splitting

function $\theta_1$ established earlier and by the fact that $\operatorname{ord}_p \sigma^k(y) = \operatorname{ord}_p y$ for any $y \in \mathbb{Q}_q$ for $k = 0, 1, ..., a-1$. $\square$

We are now ready to give an expression for the character sums $S_l^* = S_l^*(\bar{f}, q, 1, \Theta_1)$ for the case when $r = 1$. Let $G_1(x)$ be the power series defined in the above proposition corresponding to the Laurent polynomial $\bar{f}(\bar{x})$. Writing

$$\prod_{i=0}^{l-1} G_1(x^{q^i}) = \sum_{\nu} A_l(\nu) x^{\nu}$$

for some coefficiencts $A_l(\nu) \in \mathbb{Q}_q(\zeta_p)$, we have the following proposition for the case when $r = 1$.

**Proposition 2.1.26.**

$$S_l^*(q, 1, \Theta^{(1)}, \bar{f}) = (q^l - 1)^n \sum_{(q^l-1)|\nu} A_l(\nu)$$

*where the notation* $(q^l-1)|\nu$ *means that* $(q^l-1)$ *divides each component* $\nu_i$ *of the vector* $\nu \in \mathbb{Z}^n$

*Proof.* The key observation here is the fact that the map on the group of the $(q^l-1)$-th roots of unity, $\mu_{q^l-1}(\mathbb{Q}_q)$ that sends $z \mapsto z^k$ is a *multiplicative character* for any integer $k$. And this map is the trivial character if and only if $(q^l-1)|k$. And hence, we have that

$$\sum_{z^{q^l-1}=1} z^k = \begin{cases} (q^l-1) & \text{if } (q^l-1)|k \\ 0 & \text{otherwise} \end{cases}$$

Now let $V = \{\nu \in \mathbb{Z}^n : (q^l-1)|\nu\}$. Then by the previous proposition and Proposition 2.1.8 we have

$$\begin{aligned} S_l^*(q, 1, \Theta^{(1)}, \bar{f}) &= \sum_{\bar{x} \in \left(\mathbb{F}_{q^l}^{\times}\right)^n} \Theta^{(1)} \circ \tau(q, l, 1)(\bar{f}(\bar{x})) \\ &= \sum_{\substack{x_i^{q^l-1}=1 \\ 1 \le i \le n}} \prod_{j=0}^{l-1} G_1(x^{q^j}) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{x_i^{q^l-1}=1 \\ 1\le i\le n}} \sum_{\nu} A_l(\nu) x^\nu \\
&= \sum_{\nu} A_l(\nu) \sum_{\substack{x_i^{q^l-1}=1 \\ 1\le i\le n}} x^\nu \\
&= \sum_{\nu=(\nu_j)} A_l(\nu) \prod_{i=1}^{n} \sum_{x_i^{q^l-1}=1} x_i^{\nu_j} \\
&= \sum_{\nu=(\nu_j)\in V} A_l(\nu) \prod_{i=1}^{n} \sum_{x_i^{q^l-1}=1} x_i^{\nu_i} \\
&= (q^l-1)^n \sum_{(q^l-1)|\nu} A_l(\nu)
\end{aligned}
$$

□

## 2.2 The Trace Formula for the (base) case when $r = 1$

The last proposition in the previous subsection gives a nice $p$-adic expression for the character sums, $S_l^*(q, 1, \Theta^{(1)}, \bar{f})$. The goal of this subsection is to express the sum $\sum_{(q^l-1)|\nu} A_l(\nu)$ in the right hand side of the proposition as a *trace* of a certain *completely continuous endomorphism* on a certain $p$-adic Banach space. And thereby we aslo obtain an analytic expression for the associated L-function as per Definition 2.1.19. A *completely continuous endomorphism* on a $p$-adic Banach space over a $p$-adic field, $K$ is defined as a limit of finite rank continuous $K$-linear endomorphisms. A detailed account of the theory of completely continuous endomorphisms of $p$-adic Banach spaces was given by Serre [Ser62]. We will now construct a class of certain $p$-adic Banach spaces associated to the polynomial $\bar{f}$, and then show that the power series $G_1(x)$ lies in one of them on which we will later construct a completely continuous endomorphism. The theory that follows includes a generalization to Dwork's theory by Adolphson and Sperber [AS87a] through their indroduction of a Newton polyhedral weight function.

### 2.2.1 A Weight Function and certain $p$-adic Banach Spaces

Viewing the Laurent monomial $x^\nu = \prod_{i=1}^{n} x_i^{\nu_i}$ as a vector $(\nu_1, \nu_2, ..., \nu_n) \in \mathbb{Z}^n$, we may associate to every Laurent polynomial a certain monoid defined as follows. If $f \in k[x_1^{\pm}, ..., x_n^{\pm}]$ is an arbitrary Laurent polynomial over an arbitrary ring, $k$ then we may define the following:

- $Supp(f) := \{\nu \in \mathbb{Z}^n : \text{the } x^\nu \text{ term in } f \text{ has a nonzero coefficient}\}$
- $\Delta_\infty(f) :=$ The convex closure of $Supp(f) \cup \{\mathbf{0}\}$ in $\mathbb{R}^n$, where $\mathbf{0}$ is the origin
- $$Cone(f) := \begin{cases} \text{The union in } \mathbb{R}^n \text{ of all rays from the origin} \\ \text{passing through all the points in } \Delta_\infty(f), & \text{if } \Delta_\infty(f) \neq \{\mathbf{0}\} \\ \{\mathbf{0}\}, & \text{if } \Delta_\infty(f) = \{\mathbf{0}\} \end{cases}$$
  .
- $M(f) := Cone(f) \cap \mathbb{Z}^n$

Then it is clear that $M(f)$ is a monoid under addition. For any $p$-adic field, $K$, we may then define $K[[M(f)]]$ to be the collection $\{\sum_{\nu \in M(f)} A(\nu)x^\nu : A(\nu) \in K\}$ of all power series with coefficients in $K$ and support in $M(f)$. We now define a *weight function* as follows.

**Definition 2.2.1.** For each $\nu \in M(f)$, the **weight**, $w(\nu)$ is defined as the smallest nonnegative rational number, $b$ such that $\nu \in b\Delta_\infty(f) = \{v \in \mathbb{R}^n : bv \in \Delta_\infty(f)\}$.

Geometrically, the weight of a lattice point, $\nu$ represents the smallest amount by which the convex polytope, $\Delta_\infty(f)$ has to be blown up or shrunk down in order to include the the point, $\nu$. In other words, it is the smallest nonnegative rational number which is the ratio of the homothetic transformation with the origin as the centre on $\Delta_\infty(f)$ so as to include the lattice point, $\nu$. The diagram $\Delta_\infty(f)$ is called the *Newton polyhedron* of $f$,

and we call the weight function as the *Newton polyhedral weight function* associated to $f$.

The following properties of the weight function are quite evident for $\alpha, \beta \in M(f)$:

1. $w(\alpha) = 0 \iff \alpha = 0$.
2. $w(c\alpha) = cw(\alpha)$, if $c \geq 0$.
3. $w(\alpha + \beta) \leq w(\alpha) + w(\beta)$

We can, in fact, say more on the third property. Since this will be useful later on we will state it as another proposition. Before we state it let us define the notion of a *sector*. Let $d$ be the dimension of the convex polytope $\Delta_\infty(f)$. Note that $0 \leq d \leq n$ and $d = 0 \iff \Delta_\infty(f) = \{\mathbf{0}\}$ in which case its only $(d-1)$-face is the empty set. We also observe that if $\Delta_\infty(f) \neq \{\mathbf{0}\}$, then the ray from the origin passing through a point $\nu \in M(f)$ always intersects a $(d-1)$-face of $\Delta_\infty(f)$ not containing the the origin, by the definition of $\Delta_\infty(f)$. Now, for each $\nu \in M(f)$, we say that $\nu$ lies in the *sector* determined by a $(d-1)$-face, $F$ (not containing the origin) of the convex $d$-polytope $\Delta_\infty(f)$ if the ray from the origin passing through $\nu$ intersects the face at exactly one point.

**Proposition 2.2.2.** *Let $d$ be the dimension of $\Delta_\infty(f)$ and let $d > 0$. Then the following assertions hold.*

*(i) If $\mathbf{0} \neq \nu \in M(f)$ lies in the sector determined by the $(d-1)$-face, $F$ (not containing the origin) of $\Delta_\infty(f)$ whose vertices are $v_1, v_2, ..., v_m$, then there exists a subset $\{v_{i_1}, v_{i_2}, ..., v_{i_d}\}$ of $d$ linearly independent vertices such that $w(\nu) = \sum_{i=1}^{d} \alpha_i$ where $\nu = \sum_{j=1}^{d} \alpha_j v_{i_j}$ for some $\alpha_j \in \mathbb{Q}_{\geq 0}$.*

*(ii) If $d = n$ and $\nu = (\nu_1, \nu_2, ..., \nu_n) \in M(f)$ lies in the sector determined by the $(n-1)$-face, $F$ (not containing the origin) of $\Delta_\infty(f)$ contained in the supporting hyperplane defined by $l(x) = 1$ where $l(x) = l(x_1, x_2, ..., x_n) := \sum_{i=1}^{n} \lambda_i x_i$ for some $\lambda_i \in \mathbb{Q}$ is a linear form, then $w(\nu) = l(\nu) = \sum_{i=1}^{n} \lambda_i \nu_i$.*

*(iii)* *If $d \leq n$ and $\nu = (\nu_1, \nu_2, ..., \nu_n) \in M(f)$, then there exists a linear form $l(x) := \sum_{i=1}^{n} \lambda_i x_i$ with coefficients $\lambda_i \in \mathbb{Q}$ such that the hyperplane defined by $l(x) = 1$ contains a $(d-1)$-face which determines the sector in which $\nu$ lies and $w(\nu) = l(\nu) = \sum_{i=1}^{n} \lambda_i \nu_i$. And if $\tilde{l}(x)$ is any other such linear form, then we have that $\tilde{l}(\nu) = w(\nu)$ as well.*

*(iv)* *Suppose $\nu = (\nu_1, \nu_2, ..., \nu_n) \in M(f)$ and the collection $\{l_1(x), l_2(x), ..., l_k(x)\}$ of linear forms exhaustively define all the hyperplanes, $l_i(x) = 1$ containing the $(d-1)$-faces of $\Delta_\infty(f)$. Then $w(\nu) = \max\{l_1(\nu), l_2(\nu), ..., l_k(\nu)\}$. Also, if $\nu$ does not lie in the sector determined by a $(d-1)$-face contained in the hyperplane, $l_i(x) = 1$, then $w(\nu) > l_i(\nu)$.*

*(v)* *If $\mu = (\mu_1, \mu_2, ..., \mu_n), \nu = (\nu_1, \nu_2, ..., \nu_n) \in M(f)$ lie in the* same sector*, then $w(\mu + \nu) = w(\mu) + w(\nu)$, whereas if $\mu, \nu$ do not have any common sector in which both of them lie, then $w(\mu + \nu) < w(\mu) + w(\nu)$.*

*Proof.*

*Proof of Assestion (i):*

Suppose that the ray from the origin through the point $\nu$ intersects the face at the point $x$. Then we may choose $d$ linearly independent vertices $v_{i_1}, v_{i_2}, ..., v_{i_d}$, such that $x$ is a *convex* linear combination of these vectors. These vectors form a basis for the $d$-dimensional subspace of $\mathbb{R}^n$ spanned by them. Since this subspace contains the vector $\nu$, we may express the vector $\nu$ as a linear combination, $\nu = \sum_{j=1}^{d} \alpha_j v_{i_j}$. Now, since $\nu, v_{i_j} \in \mathbb{Z}^n$, the $\alpha_j \in \mathbb{Q}$. Also, the $\alpha_j$ are clearly nonnegative since the vector $\nu$ lies in the inside of the cone formed by taking the union of all the rays from the origin passing through the face, $F$. If we let $b = \sum_{j=1}^{d} \alpha_j$, then it is clear that $bx = \nu$ since $b > 0$ and $\left(\frac{1}{b}\right)\nu = \left(\frac{1}{b}\right)\sum_{j=1}^{d} \alpha_j v_{i_j}$ is the unique convex linear combination of the vertices $v_{i_j}$ that lies on the ray from the origin passing through $\nu$. Hence, $\nu \in b\Delta_\infty(f)$. And for any $0 < b' < b$, $\nu \notin b'\Delta_\infty(f)$ since $\left(\frac{1}{b'}\right)\nu \notin F$. Thus, $w(\nu) = b = \sum_{j=1}^{d} \alpha_j$.

All the remaining assertions are trivial when $\nu = \mathbf{0}$ or when $\mu = \mathbf{0}$. Hence we assume otherwise.

*Proof of Assertion (ii):*

Assertion (ii) follows from the assertion (i). By assertion (i), we may write $\nu = \sum_{k=1}^{n} \alpha_k v_k$ for some $n$ linearly independent vertices $v)k$ on the face, $F$ such that $w(\nu) = \sum_{k=1}^{n} \alpha_k$. Then, since $l(x)$ is linear and $l(v_k) = 1$ for all $k$, we have that

$$l(\nu) = l\left(\sum_{k=1}^{n} \alpha_k v_k\right) = \sum_{k=1}^{n} \alpha_k l(v_k) = \sum_{k=1}^{n} \alpha_k = w(\nu).$$

*Proof of Assertion (iii):*

From assertion (i), there are $d$ linearly independent vertices $v_1, v_2, ..., v_d$ and nonnegative rational numbers $\alpha_1, \alpha_2, ..., \alpha_d$ such that $\nu = \sum_{i=1}^{d} \alpha_i v_i$, and $w(\nu) = \sum_{i=1}^{d} \alpha_i$. The vectors $v_1, v_2, ..., v_d$ can be extended to a set $T = \{v_1, v_2, ..., v_n\}$ that forms a basis for $\mathbb{Q}^n$, and observe that $T$ is also a basis for $\mathbb{R}^n$. Since the set $T = \{v_1, v_2, ..., v_n\}$ is linearly independent, it is also *affinely* independent as set of *points* And thus, the set of *vectors* $S = \{v_2 - v_1, v_3 - v_1, ..., v_n - v_1\}$ is linearly independent (please see lemma (a standard fact) below). Hence, the *affine* span of the set of points, $T$ has dimension $(n-1)$.

**Lemma 2.2.3.** *Recall that a set of points $v_1, v_2, ..., v_k$ in the vector space $\mathbb{R}^n$ are said to be* affinely independent *if whenever a linear combination $c_1v_1 + c_2v_2 + ... + c_kv_k = 0$ with $\sum_{i=1}^{k} c_i = 0$, then $c_i = 0$ for all $i = 1, 2, ..., k$. Also, the* affine span *of such a set of points the smallest affine space containing them.*

*Let $T$ be a set of points $\{v_1, v_2, ..., v_k\} \in \mathbb{R}^n$. Then $T$ is affinely independent if and only if the set of* vectors

$$S = \{v_2 - v_1, v_3 - v_1, ..., v_k - v_1\}$$

*is linearly independent in $\mathbb{R}^n$.*

*Proof.* This is a straightforward argument. Please see Appendix B. □

Since the *linear* span of $S$, call it $W$, has dimension $(n-1)$, its orthogonal complement, $W^{\perp}$ is a one dimensional subspace of $\mathbb{R}^n$. Let $u$ be a generator of $W^{\perp}$. We may

choose $u \in \mathbb{Q}^n$, since $W$ and $W^\perp$ can also be viewed as subspaces of $\mathbb{Q}^n$. Then it is clear that the hyperplane containing the points in $T$ has an equation given by

$$(x - v_1) \cdot u = 0$$

where $\cdot$ represents the dot product in $\mathbb{R}^n$. It is also evident that $v_1 \cdot u \neq 0$, for otherwise the basis $T$ is orthogonal to a nonzero vector $u$, which is absurd. Hence, the above equation can be rewritten as an equation of the form,

$$l(x) := \sum_{i=1}^{n} \lambda_i x_i = 1$$

for some coefficients $\lambda_i \in \mathbb{Q}$.

Now, since $l(x)$ is linear and $l(v_i) = 1$ for $i = 1, 2, ..., d$, we have that

$$l(\nu) = l\left(\sum_{i=1}^{d} \alpha_i v_i\right) = \sum_{i=1}^{d} \alpha_i l(v_i) = \sum_{i=1}^{d} \alpha_i = w(\nu).$$

and by the same argument, $\tilde{l}(\nu) = w(\nu)$ if $\tilde{l}(x)$ is any other such form.

*Proof of Assertion (iv):*

Assertion (iv) follows from the simple observation that the point of intersetion (if it exists) of the ray from the origin passing through $\nu$ with the hyperplane defined by $l_i(x) = 1$ is given by $\dfrac{\nu}{l_i(\nu)}$ and hence the distance from the origin to this point of intersection is $\dfrac{\|\nu\|}{l_i(\nu)}$. Then it is clear from the convexity of $\Delta_\infty(f)$ that this distance is the least when the hyperplane, $l_i(x) = 1$ contains a $(d-1)$-face which determines a sector in which $\nu$ lies in, and stritcly larger than the minimum when it does not contain a face determining one of its sectors. And thus assertion (iv) follows from assertion (iii). (If the point of intersection does not exist, then $l_i(\nu) \leq 0 \leq w(\nu)$).

*Proof of Assertion (v):*

The first part of assertion (v) follows from assersions (i), (ii) and (iii) since the vector $\mu + \nu$ lies in the same sector as well. Finally suppose $\mu$ and $\nu$ do not have any common sector in which both of them lie, and suppose that $w(\mu + \nu) = l_*(\mu + \nu)$ for some linear

form $l_*(x)$ as per assertion (iii). Then by the hypothesis and by assertion (iv), at least one of the strict inequalities: $l_*(\mu) < w(\mu), l_*(\nu) < w(\nu)$ must hold. It follows that $w(\mu+\nu) = l_*(\mu+\nu) = l_*(\mu) + l_*(\nu) < w(\mu) + w(\nu)$. □

**Corollary 2.2.4.** *For $\nu \in M(f)$, $w(\nu) = \inf\left\{ \sum_{\mu \in Supp(f)} r_\mu : \sum_{\mu \in Supp(f)} r_\mu \mu = \nu, r_\mu \in \mathbb{Q}_{\geq 0} \right\}$.*

*Proof.* Since for $r_\mu \in \mathbb{Q}_{\geq 0}$ we have

$$w\left( \sum_{\mu \in Supp(f)} r_\mu \mu \right) \leq \sum_{\mu \in Supp(f)} r_\mu w(\mu) = \sum_{\mu \in Supp(f)} r_\mu$$

it is clear that $w(\nu)$ is less than or equal to the infimum. On the other hand, $w(\nu)$ is greater than or equal to the infimum by the above proposition. □

**Corollary 2.2.5.** *Let $d$ be the dimension of $\Delta_\infty(f)$. There exists a positive integer $D$ such that for all $\nu \in M(f)$, $w(\nu) \in \left(\frac{1}{D}\right)\mathbb{Z}$.*

*Proof.* The rational coefficients of a linear form $\sum_{i=1}^{n} \lambda_i x_1$ as in assertion (iii) in the previous proposition have a common denominator. Moreover, there are only finitely many $(d-1)$-faces. We may choose $D$ to be the least common multiple of the common denominators of the rational coefficients of certain linear forms corresponding to each of the $(d-1)$-face as in assertion (iii). □

Now let $\bar{f}$ be the polynomial as in subsection 2.1.3. Let us define certain $p$-adic Banach spaces associated to $\bar{f}$ as follows. For each rational number $b \geq 0$, given a $p$-adic field, $K$, we may define the collection of formal power series,

$$B_{\bar{f}}(b, K) := \left\{ \sum_{\nu \in M(\bar{f})} A(\nu) x^\nu : A(\nu) \in K, \inf_{\nu \in M(\bar{f})} \{ \mathrm{ord}_p A(\nu) - w(\nu) b \} > -\infty \right\}.$$

Furthermore, writing $b = \frac{c}{d}$ for some coprime positive integers $c, d$, we could choose a $p$-adic field, $K_{\bar{f},b}$ such that there exists an element $\pi_b \in K_{\bar{f},b}$ with $\mathrm{ord}_p \pi_b = b$ and $\pi_b^{w(\nu)} \in K_{\bar{f},b}$ for all $\nu \in M(\bar{f})$. For example, we may choose $K_{\bar{f},b}$ to be the field obtained by adjoining a root of the Eisenstein polynomial, $x^{dD} - p$ to $\mathbb{Q}_p$ where $D$

is a positive integer as in Corollory 2.2.5, so that $K_{\bar{f},b}$ is a totally ramified extension of $\mathbb{Q}_p$ of degree $dD$. Hence, if the field $K$ is appropriately chosen, then any element $\xi = \xi(x) = \sum_{\nu \in M(\bar{f})} A(\nu)x^\nu \in B_{\bar{f}}(b, K)$ can be rewritten (uniquely) as

$$\xi(x) = \sum_{\nu \in M(\bar{f})} A(\nu)x^\nu = \sum_{\nu \in M(\bar{f})} \tilde{A}(\nu)\pi_b^{w(\nu)}x^\nu \tag{2.2.1}$$

for some coefficients $\tilde{A}(\nu) \in K$. Now since $\inf_{\nu \in M(\bar{f})} \{\mathrm{ord}_p A(\nu) - w(\nu)b\} > -\infty$, there exists a real number $e$ such that $\mathrm{ord}_p A(\nu) - w(\nu)b \geq e$ for all $\nu \in M(\bar{f})$ or equivalently, $\mathrm{ord}_p \tilde{A}(\nu) \geq e$ for all $\nu \in M(\bar{f})$. Thus, for an appropriately chosen $K$, the collection $B_{\bar{f}}(b, K)$ can be viewed as a *p-adic Banach space* over $K$ isomorphic to the collection of all bounded sequences $(\tilde{A}(\nu))_{\nu \in M(\bar{f})}$ of elements of $K$ indexed by the countable collection, $I = \{\pi_b^{w(\nu)}x^\nu : \nu \in M(\bar{f})\}$ under the norm, $|\cdot|$ defined by $|\xi| := \sup_{\nu \in M(\bar{f})} |\tilde{A}(\nu)|_p$. In Serre's terminology [Ser62], this is the space $b_{M(\bar{f})}(K)$, the space of bounded sequences in $K$ indexed by the elements of the countable set, $M(\bar{f})$. While it is true that the set $I$ is linearly independent and that $|\xi| = 1$ for every $\xi \in I$, it is *not* a basis in any sense since the series in the unique representation as a *formal sum* in Equation 2.2.1 is not convergent with respect to the norm. However, if the valuation of $K$ is discrete, then the set $I$ is an *orthonormal basis* for the closed subspace, $C_{\bar{f}}(b, K) \subset B_{\bar{f}}(b, k)$ consisting of sequences $(\tilde{A}(\nu))_{\nu \in M(\bar{f})}$ that converge to zero with respect to the cofinite filter on $M(\bar{f})$, (with respect to the same norm). In other words, $C_{\bar{f}}(b, K)$ is isometrically isomorphic to the $c(M(\bar{f}))$ space in Serre's terminology [Ser62].

We will, from now onwards, suppress the field $K$ in our notation $B_{\bar{f}}(b, K)$ (resp. $C_{\bar{f}}(b, K)$) and write $B_{\bar{f}}(b)$ (resp. $C_{\bar{f}}(b)$) instead to denote these Banach spaces. And when we talk about relationships between multiple Banach spaces of this kind, we understand that the field $K$ was chosen a priori so that all the notations make sense. We will always choose $K$ so that $\mathbb{Q}_q(\zeta_p) \subset K$. However, we insist that the field $K$ is always discretely valued as opposed to assuming that $K = \mathbb{C}_p$ for the remainder of this paper, the reason being that only then we could apply certain results from [Ser62].

We will now state some important properties of the Banach space $B_{\bar{f}}(b)$ and its closed subspace $C_{\bar{f}}(b)$. These properties will be used in the proof of a crucial proposition given

below. We first observe that $B_{\bar{f}}(b)$ is a Banach space satisfying the property that for every $\xi \in B_{\bar{f}}(b)$, $|\xi| \in \overline{|K|}$, where $\overline{|K|}$ is the closure of the value group of $K$. That is, $B_{\bar{f}}(b)$ satisfies condition (N) in Serre's terminology ([Ser62]). In other words, the norm on $B_{\bar{f}}(b)$ is a *solid* norm in the terminology of [PGS10]. Also since the valuation of $K$ is discrete, it follows that $B_{\bar{f}}(b)$ is isometrically isomorphic to a $c(J)$ space (in Serre's terminology) for some set $J$, which is necessarily uncountable ([PGS10]: Theorem 2.5.15). As pointed out earlier, the collection $I$ is an orthonormal basis for the closed subspace $C_{\bar{f}}(b)$. In particluar, $I$ is an orthonormal system of the space $B_{\bar{f}}(b)$ in the teminology of [PGS10]. We also note that the set $I$ can be extended to an orthonormal basis $J \supset I$ of $B_{\bar{f}}(b)$ ([PGS10]: Lemma 8.1.11).

**Proposition 2.2.6.** *For rational numbers $b' > b \geq 0$, the inclusion map $\mathbf{i} : B_{\bar{f}}(b') \hookrightarrow B_{\bar{f}}(b)$ is completely continuous.*

*Proof.* Let $\pi_{b'}, \pi_b \in K$ be chosen such that $\operatorname{ord}_p \pi_{b'} = b'$ and $\operatorname{ord}_p \pi_b = b$ and hence $I' := \{\pi_{b'}^{w(\nu)} x^\nu : \nu \in M(\bar{f})\}$ and $I := \{\pi_b^{w(\nu)} x^\nu : \nu \in M(\bar{f})\}$ are orthonormal systems in $B_{\bar{f}}(b')$ and $B_{\bar{f}}(b)$ respectively, such that $B_{\bar{f}}(b')$ and $B_{\bar{f}}(b)$ are isometrically isomorphic to the Banach spaces $b(I')$ and $b(I)$ respectively (in Serre's terminology). Now let $J' \supset I'$ and $J \supset I$ be the extensions of these orthonormal systems to orthonormal bases for these spaces respectively, such that $B_{\bar{f}}(b')$ and $B_{\bar{f}}(b)$ are isometrically isomorphic to the Banach spaces $c(J')$ and $c(J)$ respectively (in Serre's terminology). We note that $I$ is countable, $J$ is uncountable and the closed subspaces $C_{\bar{f}}(b')$ and $C_{\bar{f}}(b)$ of $B_{\bar{f}}(b')$ and $B_{\bar{f}}(b)$ respectively are isometrically isomorphic to the Banach spaces $c(I')$ and $c(I)$ respectively.

Let us now describe the *matrix* (as described in [Ser62]) of the inclusion map $\mathbf{i} : B_{\bar{f}}(b') \hookrightarrow B_{\bar{f}}(b)$ with respect to the *orthonormal bases* $J'$ and $J$ by first looking at the action of $\mathbf{i}$ on each of the elements in the basis $J'$. Note that here we use the convention of treating the elements of $B_{\bar{f}}(b')$ as *column vectors* and thus the matrix is multiplied from the left of the column vector. This is the opposite of Serre's convention where he treats the elements as *row vectors* and defines the matrix accordingly.

Let $M = (M_{jj'})$ denote the matrix so that for any $\xi = \sum_{j'} C_{j'} j'$, $\mathbf{i}(\xi)$ is given by

$\mathbf{i}(\xi) = \sum_j \sum_{j'} M_{jj'} C_{j'} j$, that is, $\mathbf{i}(\xi) = (D_j)_{j \in J}$ where $D_j = \sum_{j'} M_{jj'} C_{j'}$.

Now, if $j' \in J'$, there are two cases: either $j' \in I'$ or $j' \in J' - I'$.

In the former case, $j' = \pi_{b'}^{w(\nu)} x^\nu$ for some $\nu \in M(\bar{f})$. Then $\mathbf{i}(j') = \pi_{b'}^{w(\nu)} x^\nu = \left(\frac{\pi_{b'}^{w(\nu)}}{\pi_b^{w(\nu)}}\right) \pi_b^{w(\nu)} x^\nu$. Thus, $\mathbf{i}(j')$ has only one nonzero coefficient with respect to the orthonormal basis $J$ and we see that in fact, $\mathbf{i}(j') \in C_{\bar{f}}(b)$. We conclude that in the former case, $M_{jj'} = 0$ for all $j \in J$ except one $j \in I \subset J$, call it $j_{j'}$, for which $M_{j_{j'}j'} = \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu)}$. Observe carefully that the $I', I$ and $M(\bar{f})$ are in bijection with each other. We write $\nu_{j'}$ to denote the image of $j'$ under the bijection from $I'$ onto $M(\bar{f})$, and similarly, we write $\nu_j$ to denote the image of $j$ under the bijection from $I$ onto $M(\bar{f})$ and $\boxed{j' = \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_j)} j}$ when $j \in I$, and hence there is no possible confusion. We also observe that $\mathbf{i}(C_{\bar{f}}(b')) \subset C_{\bar{f}}(b)$ since $\operatorname{ord}_p M_{jj'} = w(\nu_j)(b' - b)$ which tends to $\infty$ as $j \to \infty$ with respect to the cofinite filter on $J$.

On the other hand, in the latter case when $j' \notin I'$, then since $|j'| = 1$, we may write $\boxed{j' = \sum_{i' \in I'} \tilde{A}_{j'}(\nu_{i'}) \pi_{b'}^{w(\nu_{i'})} x^{\nu_{i'}}}$ for some $\tilde{A}_{j'}(\nu_{i'}) \in K$ such that $\operatorname{ord}_p \tilde{A}_{j'}(\nu_{i'}) \geq 0$. Then,

$$\begin{aligned}
\mathbf{i}(j') &= \mathbf{i}\left[\sum_{i' \in I'} \tilde{A}_{j'}(\nu_{i'}) \pi_{b'}^{w(\nu_{i'})} x^{\nu_{i'}}\right] \\
&= \sum_{i \in I} \tilde{A}_{j'}(\nu_i) \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_i)} \pi_b^{w(\nu_i)} x^{\nu_i} \\
&= \sum_{i \in I} \tilde{D}_{j'}(\nu_i) \pi_b^{w(\nu_i)} x^{\nu_i}
\end{aligned}$$

where $\boxed{\tilde{D}_{j'}(\nu_i) = \tilde{A}_{j'}(\nu_i) \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_i)}}$. Now since $\operatorname{ord}_p \left[\tilde{A}_{j'}(\nu_i) \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_i)}\right] \geq w(\nu_i)(b' - b)$ which tends to $\infty$ as $i \to \infty$, it follows that $\mathbf{i}(j') \in C_{\bar{f}}(b)$ in this case as well. Hence, $\mathbf{i}(j') \in C_{\bar{f}}(b)$ for all $j' \in J'$, and thus we have

$$\boxed{M_{jj'} = 0 \quad \text{if } j \notin I}.$$

and we have proved that the range of the inclusion operator, $\mathbf{i}$ is $C_{\bar{f}}(b)$ which is of countable dimension.

Now fix $j \in I$. We have,

$$M_{jj'} = \begin{cases} \tilde{A}_{j'}(\nu_j)\left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_j)} & \text{if } j' \in J' - I' \\ \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_j)} & \text{if } j' \in I' \text{ and } \nu_{j'} = \nu_j \\ 0 & \text{if } j' \in I' \text{ and } \nu_{j'} \neq \nu_j \end{cases}.$$

from which we infer that $\boxed{w_j := \inf_{j' \in J'} \{\mathrm{ord}_p\, M_{jj'}\} = w(\nu_j)(b' - b)}$ since $\mathrm{ord}_p\, \tilde{A}_{j'}(\nu_j) \geq 0$.

We thus deduce that $\mathbf{i}$ is completely continuous as we see that $w_j \to \infty$ as $j \to \infty$ with respect to the cofinite filter on the $J$. The matrix, $M$ of $\mathbf{i}$ is shown below for additional clarity. It has four blocks.

$$M = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$$

where $C = D = \mathbf{0}$, the rows of $A$ are indexed by $I$, the rows of $C$ are indexed by $J - I$, the columns of $A$ are indexed by $I'$ and the columns of $B$ are indexed by $J' - I'$. $A$ is a *diagonal* matrix with $A_{jj'} = \left(\frac{\pi_{b'}}{\pi_b}\right)^{w(\nu_j)}$ if $\nu_j = \nu_{j'}$ and is 0 otherwise. And the entries of $B$ are given by $B_{jj'} = \tilde{D}_{j'}(\nu_j)$ which was defined earlier. $\square$

Now observe that the space $B_{\bar{f}}(b)$ can be expressed in terms of smaller subspaces, $B_{\bar{f}}(b, c)$ for real numbers $c$ as follows. Define

$$B_{\bar{f}}(b,c) := \left\{ \sum_{\nu \in M(\bar{f})} A(\nu)x^{\nu} : A(\nu) \in K, \operatorname{ord}_p A(\nu) \geq w(\nu)b + c \right\}$$

so that $B_{\bar{f}}(b) = \bigcup_{c \in \mathbb{R}} B_{\bar{f}}(b,c)$. Then the following lemma holds.

**Lemma 2.2.7.** *Let $b$ be a nonnegative rational number and let $c, c'$ be real numbers. Then the following assertions hold.*

1. $B_{\bar{f}}(b,c)B_{\bar{f}}(b,c') \subset B_{\bar{f}}(b,c+c')$
2. *If $\xi(x) \in B_{\bar{f}}(b,c)$, then $\xi(x^p) \in B_{\bar{f}}(b/p,c)$*
3. *If rational numbers $b' > b > 0$, then $B_{\bar{f}}(b',c) \subset B_{\bar{f}}(b,c)$*

*Proof.* If $\xi = \sum_{\omega \in M(\bar{f})} D(\omega)x^{\omega} \in B_{\bar{f}}(b,c)$ and $\xi' = \sum_{\omega \in M(\bar{f})} D'(\omega)x^{\omega} \in B_{\bar{f}}(b,c')$, then

$$\xi\xi' = \sum_{\omega \in M(\bar{f})} \left( \sum_{\mu+\nu=\omega} D(\mu)D'(\nu) \right) x^{\omega}$$

and the sum $E(\omega) := \sum_{\mu+\nu=\omega} D(\mu)D'(\nu)$ converges since $\operatorname{ord}_p D(\mu) \to \infty$ as $\mu \to \infty$ and the collection $\{D'(\nu) : \nu \in M(\bar{f}), \operatorname{ord}_p D(\nu) \geq w(\nu)b + c'\}$ is bounded $p$-adically. And,

$$\begin{aligned} \operatorname{ord}_p E(\omega) &\geq \inf_{\mu+\nu=\omega} \{w(\mu)b + c + w(\nu)b + c'\} \\ &\geq (w(\mu) + w(\nu))b + c + c' \\ &\geq w(\omega)b + c + c' \end{aligned}$$

where the second inequality holds for all $\mu, \nu \in M(\bar{f})$ such that $\mu + \nu = \omega$ and the last inequality is due to the property of the weight function. Statement (2) follows from the fact that $w(p\omega) = pw(\omega)$ for $\omega \in M(\bar{f})$ and statement (3) is trivial. Hence we have the lemma. □

**Corollary 2.2.8.** *The series* $G_1(x) = \prod_{i=0}^{a-1} F^{\sigma^i}(x^{p^i}) \in B_{\bar{f}}\left(\frac{p}{q(p-1)}, 0\right) \subset B_{\bar{f}}\left(\frac{p}{q(p-1)}\right)$.

*Proof.* We first observe that $F(x) = \prod_{\mu \in Supp(\bar{f})} \theta_1(a_\mu x^\mu) \in B_{\bar{f}}\left(\frac{1}{p-1}, 0\right)$. Writing $\theta_1(t) = \sum_{m=0}^{\infty} b_m t^m$ for some coefficients $b_m$ satisfying $\mathrm{ord}_p\, b_m \geq \frac{m}{p-1}$ (recall the proof of Proposition 2.1.13), we may write

$$\begin{aligned} F(x) &= \prod_{\mu \in Supp(\bar{f})} \sum_{m_\mu=0}^{\infty} b_{m_\mu} (a_\mu x^\mu)^{m_\mu} \\ &= \sum_{\nu \in M(\bar{f})} C(\nu) x^\nu \end{aligned}$$

for some coefficients $C(\nu)$ given by $C(\nu) = \sum \prod_{\mu \in Supp(\bar{f})} b_{m_\mu} A_\mu^{m_\mu}$ with the sum running over nonnegative linear combinations $\sum_{\mu \in Supp(\bar{f})} m_\mu \mu$ such that $\sum_{\mu \in Supp(\bar{f})} m_\mu \mu = \nu$ for each $\nu \in M(\bar{f})$. Then we have

$$\begin{aligned} \mathrm{ord}_p\, C(\nu) &\geq \inf_{\sum m_\mu \mu = \nu} \left\{ \mathrm{ord}_p \prod_{\mu \in Supp(\bar{f})} b_{m_\mu} a_\mu^{m_\mu} \right\} \\ &\geq \inf \left\{ \frac{1}{p-1} \sum_{\mu \in Supp(\bar{f})} m_\mu : \sum m_\mu \mu = \nu, m_\mu \in \mathbb{Z}_{\geq 0} \right\} \\ &\geq \inf \left\{ \frac{1}{p-1} \sum_{\mu \in Supp(\bar{f})} m_\mu : \sum m_\mu \mu = \nu, m_\mu \in \mathbb{Q}_{\geq 0} \right\} \\ &= \left( \frac{1}{p-1} \right) w(\nu) \end{aligned}$$

where the second inequality is due to the fact that the $a_\mu$ are Teichmüller *units* and the last equality follows from Corollory 2.2.4. Hence $F(x) \in B_{\bar{f}}\left(\frac{1}{p-1}, 0\right)$. Then it is clear that $F^{\sigma^i}(x^{p^i}) \in B_{\bar{f}}\left(\frac{1}{p^i(p-1)}, 0\right)$ for $i = 1, 2, ..., a-1$ from the above lemma and the result follows from the lemma again. □

**Remark 2.2.9.** An important point to be noted is the fact that the splitting function $\theta_1(t)$ converges $p$-adically on a disk of radius *greater* than 1 as established in Proposition 2.1.4. This *overconvergence* of $\theta_1(t)$ was crucial in the above proof in establishing that

$$F(x) \in B_{\bar{f}}\left(\frac{1}{p-1}, 0\right)$$

because the overconvergence followed from the fact that

$$\operatorname{ord}_p b_m \geq \frac{m}{p-1}$$

when $\theta_1(t)$ is written as $\theta_1(t) = \sum_{m=0}^{\infty} b_m t^m$. Only because of the overconvergence, we have that $F(x) \in B_{\bar{f}}(b)$ for some *positive* $b$. We will see, in what follows, that the property that $F(x) \in B_{\bar{f}}(b)$ for some $b > 0$ is crucial in the construction of a certain *completely continuous* endomorphism on $B_{\bar{f}}(b)$.

### 2.2.2 The Frobenius and the Trace Formula

We are now ready to state the trace formula and then later express the L-function in terms of a Frobenius map acting on a certain Koszul complex. Let us first define the $\psi_q$ linear operator which plays a fundamental role. Let $b$ be a nonnegative rational number. For $\xi(x) = \sum_{\omega \in M(\bar{f})} C(\omega)x^{\omega} \in B_{\bar{f}}(b, c)$, we define $\psi_q : B_{\bar{f}}(b, c) \to B_{\bar{f}}(qb, c)$ by $\psi_q(\xi(x)) := \sum_{\substack{\omega \in M(\bar{f}) \\ q|\omega}} C(\omega)x^{q^{-1}\omega} = \sum_{\nu \in M(\bar{f})} C(q\nu)x^{\nu}$. We note that $\operatorname{ord}_p C(q\nu) \geq w(q\nu)b + c = w(\nu)qb + c$, hence the map is well defined. Also, this map is a bounded (therefore, continuous) $K$-linear operator on $B_{\bar{f}}(b)$, since given a basis, $\{\pi_b^{w(\nu)} x^{\nu} : \nu \in M(\bar{f})\}$ for $B_{\bar{f}}(b)$, we may take the set $\{\pi_b^{qw(\nu)} x^{\nu} : \nu \in M(\bar{f})\}$ to be the basis for $B_{\bar{f}}(qb)$. We also observe that for $H \in B_{\bar{f}}(b)$, the operator, "multiplication by $H$", $H : B_{\bar{f}}(b) \to B_{\bar{f}}(b)$ defined by $H(F) := HF$ is a continuous $\mathbb{C}_p$-linear map (recall Lemma 2.2.7). Then by Proposition 2.2.6, and by the fact that the composition of a continuous linear operator with a completely continuous linear operator is completely continuous [Ser62], we have that whenever $b > 0$, the composite, $i_q \circ \psi_q \circ H : B_{\bar{f}}(b) \to B_{\bar{f}}(b)$

$$B_{\bar{f}}(b) \xrightarrow{H} B_{\bar{f}}(b) \xrightarrow{\psi_q} B_{\bar{f}}(qb) \xrightarrow{i_q} B_{\bar{f}}(b)$$

completely continuous, where $i_q$ is the inclusion map. We now apply the crucial result

from Serre (Corollory 3 in Section 5 in [Ser62]). The operator $\alpha : B_{\bar{f}}(b) \to B_{\bar{f}}(b)$ defined by $\alpha := i_q \circ \psi_q \circ G_1$, where $b = \dfrac{p}{q(p-1)}$ and $G_1(x) = \prod_{i=0}^{a-1} F^{\sigma^i}(x^{p^i})$ is completely continuous on the $p$-adic Banach space, $B_{\bar{f}}(b)$ over the discretely valued field $K$ of charecteristic zero. Hence,

$$\det(\mathbb{I} - t\alpha) = \exp\left(-\sum_{m=1}^{\infty} \frac{\mathrm{Tr}(\alpha^m)t^m}{m}\right) \tag{2.2.2}$$

where $\mathbb{I}$ is the identity endomorphism. And in particular, the trace, $\mathrm{Tr}(\alpha^m)$ is defined for $m \in \mathbb{Z}_{\geq 0}$ since the $\alpha^m$ are all completely continuous and hence they are of trace-class [Ser62].

**Lemma 2.2.10.** *Let $B$ be an arbitrary Banach space over a non-Archimedian discretely valued field, $k$ which is complete with respect to the valuation. Suppose that $B$ is isometrically isomorphic to a $c(I)$ space for some* ***countable*** *set $I$ in the sense of [Ser62]. That is, $B$ is the space of all sequences $(x_i)_{i\in I}$ of elements of $k$ which converge to zero with respect to the cofinite filter on $I$. Let $J = \{e_i\}_{i\in I} \subset B$ be the orthonormal basis for $B$. Let $\beta : B \to B$ be a completely continuous endomorphism of $B$. Suppose that the matrix of $\beta$ with respect to the orthonormal basis, $J$ is given by $(A_{ij})$ (in the sense of [Ser62]). Let $J' = \{c_i e_i\}_{i\in I}$ for some arbitrary nonzero scalars $c_i \in k$. Then the matrix of $\beta$ with respect to the Schauder basis (in the sense of [PGS10]), $J'$ is given by $((c_i c_j^{-1})A_{ij})$. And hence the trace of $\beta$ can be computed with respect to the basis, $J'$.*

*Proof.* It is clear that $J'$ is a topological basis (in the sense of [PGS10]) since it is countable and every $x \in B$ can be written uniquely as a sum $x = \sum_{i\in I} \lambda_i c_i e_i$ for some $\lambda_i \in k$. Also, it is a Schauder basis by Theorem 2.3.11 in [PGS10]. The rest of the proof trivially follows from the observation that

$$\begin{aligned}
\beta(c_i e_i) &= \sum_{j\in I} A_{ij} c_i e_j \\
&= c_i \sum_{j\in I} c_j^{-1} A_{ij} c_j e_j \\
&= \sum_{j\in I} (c_i c_j^{-1}) A_{ij} (c_j e_j).
\end{aligned}$$

□

**Proposition 2.2.11.** *Let $b$ be a positive rational number. If $H(x) = \sum_{\omega \in M(\bar{f})} A(\omega)x^{\omega} \in B_{\bar{f}}(b)$, then the trace,*

$$\mathrm{Tr}(i_q \circ \psi_q \circ H) = \sum_{\substack{\nu \in M(\bar{f}) \\ (q-1)|\nu}} A(\nu) = \sum_{\nu \in M(\bar{f})} A((q-1)\nu)$$

*Proof.* Let $\beta = (i_q \circ \psi_q \circ H)$. Let us first compute the trace of $\beta|_{C_{\bar{f}}(b)}$, the restriction of $\beta$ to the closed subspace $C_{\bar{f}}(b)$ of $B_{\bar{f}}(b)$. We observe that this restriction is *stable* on the subspace. This is because, if $\xi \in C_{\bar{f}}(b)$, then $\beta(\xi) \in B_{\bar{f}}(qb) \subset C_{\bar{f}}(b)$. The last inclusion is justified by the following reasoning. If $\pi_b \in K$ is an element satisfying $\mathrm{ord}_p \pi_b = b$, then we may consider the collection $I_b = \{\pi_b^{w(\nu)} x^{\nu} : \nu \in M(\bar{f})\}$ as an orthonormal system in $B_{\bar{f}}(b)$ such that $B_{\bar{f}}(b)$ is isometrically isomorphic to the space $b(I_b)$. Now, set $\pi_{qb} = \pi_b^q$ so that $\mathrm{ord}_p \pi_{qb} = qb$. Then the collection $I_{qb} = \{\pi_{qb}^{w(\nu)} x^{\nu} : \nu \in M(\bar{f})\}$ as an orthonormal system in $B_{\bar{f}}(qb)$ such that $B_{\bar{f}}(qb)$ is isometrically isomorphic to the space $b(I_{qb})$. Now if $\eta \in B_{\bar{f}}(qb)$, then we may write $\eta$ as a formal sum

$$\eta = \sum_{\nu \in M(\bar{f})} D(\nu)\pi_{qb}^{w(\nu)} x^{\nu}$$

for some coefficients $D(\nu)$ such that $\mathrm{ord}_p D(\nu) \geq e$ for some $e \in \mathbb{R}$. Then we have

$$\eta = \sum_{\nu \in M(\bar{f})} D(\nu)\pi_b^{(q-1)w(\nu)} \pi_b^{w(\nu)} x^{\nu} \in C_{\bar{f}}(b)$$

because $\mathrm{ord}_p \left[ D(\nu)\pi_b^{(q-1)w(\nu)} \right] \geq e + (q-1)w(\nu) \to \infty$ as $\nu \to \infty$. Hence, the restriction $\beta|_{C_{\bar{f}}(b)}$ is a completely continuous *endomorphism* of $C_{\bar{f}}(b)$.

Then the trace, $\mathrm{Tr}(\beta|_{C_{\bar{f}}(b)})$ can be computed from a matrix representation of the map, $i_q \circ \psi_q \circ H$ with respect to the Schauder basis (in the sense of [PGS10]), $\{x^{\nu} : \nu \in M(\bar{f})\}$ due to Lemma 2.2.10. To see this, consider an element $\pi_b \in B_{\bar{f}}(b)$ such that

$\operatorname{ord}_p \pi_b = b$ and so that the collection, $I = \{\pi_b^{w(\nu)} : \nu \in M(\bar{f})\}$ is an orthonormal system for $B_{\bar{f}}(b)$ such that $B_{\bar{f}}(b)$ is isometrically isomorphic to the space, $b(I)$ of all bounded sequences of elements of $K$ indexed by the set, $I$. Then, $I$ is an *orthonormal basis* for the closed subspace $C_{\bar{f}}(b)$.

Now, suppose that the matrix, $M$ of the map with respect to the basis $\{x^\nu :: \nu \in M(\bar{f})\}$ is given by $M = [M_{\nu\mu}]$, so that we have

$$(i_q \circ \psi_q \circ H)(x^\mu) = \sum_{\nu \in M(\bar{f})} a_{\nu\mu} x^\nu$$

On the other hand, the action of the map on the basis element $x^\mu$ is given by

$$\begin{aligned}(i_q \circ \psi_q \circ H)(x^\mu) &= \psi_q \left( \sum_{\omega \in M(\bar{f})} A(\omega) x^{\omega+\mu} \right) \\ &= \sum_{\substack{\omega \in M(\bar{f}) \\ q|(\omega+\mu)}} A(\omega) x^{\left(\frac{\omega+\mu}{q}\right)}\end{aligned}$$

Hence we must have that $M_{\nu\mu} = A(q\nu - \mu)$. And thus the trace is given by

$$\operatorname{Tr}(\beta|_{C_{\bar{f}}(b)}) = \sum_{\nu \in M(\bar{f})} a_{\nu\nu} = \sum_{\nu \in M(\bar{f})} A\left((q-1)\nu\right). \tag{2.2.3}$$

Finally, on extending the orthonormal system $I$ to an orthormal basis $J$ for the space, $B_{\bar{f}}(b)$, it is not hard to see that the trace of $\beta$ with respect to the orthonormal basis $J$ should coincide with the right hand side of Equation 2.2.3, which is the expression for the trace of $\beta|_{C_{\bar{f}}(b)}$ with respect to the orthonormal basis $I$. This is because any basis element $\xi \in J - I$ is of the form $\xi = \sum_{\lambda \in M(\bar{f})} D(\lambda) \pi_b^{w(\lambda)} x^\lambda$ with the coefficients $D(\lambda)$ satisfying $\operatorname{ord}_p D(\lambda) \geq 0$. Then the sequence $(E(\lambda))_{\lambda \in M(\bar{f})}$ where $E(\lambda) = D(\lambda)\pi_b^{w(\lambda)}$ can be viewed as an element in the Banach space $c(I')$ indexed by $I' = \{x^\lambda : \lambda \in M(\bar{f})\}$ which is also an orthonormal basis, since $\operatorname{ord}_p E(\lambda) \to \infty$ as $\lambda \to \infty$. Then $\beta(\xi)$ can be computed by the same matrix, $M$ as above, with this point of view. And since $\beta$ is

linear, its trace, $\mathrm{Tr}(\beta)$ must coincide with the expression given by the right hand side of Equation 2.2.3. □

**Lemma 2.2.12.** *Let $b$ be a nonnegative rational number. If $a(x) = \sum_{\mu \in M(\bar{f})} A(\mu)x^{\mu}, b(x) = \sum_{\nu \in M(\bar{f})} B(\nu)x^{\nu} \in B_{\bar{f}}(b)$, then*

$$\psi_q\left(a(x^q)b(x)\right) = a(x)\psi_q\left(b(x)\right).$$

*Proof.* This follows from the $K$-linearity of the $\psi_q$ operator. We have:

$$\begin{aligned}
\psi_q(a(x^q)b(x)) &= \psi_q\left(\sum_{\mu \in M(\bar{f})} A(\mu)x^{q\mu}b(x)\right) \\
&= \sum_{\mu \in M(\bar{f})} A(\mu)\psi_q\left(x^{q\mu}b(x)\right) \\
&= \sum_{\mu \in M(\bar{f})} A(\mu)\psi_q\left(x^{q\mu}\sum_{\nu \in M(\bar{f})} B(\nu)x^{\nu}\right) \\
&= \sum_{\mu \in M(\bar{f})} A(\mu)\psi_q\left(\sum_{\nu \in M(\bar{f})} B(\nu)x^{\nu+q\mu}\right) \\
&= \sum_{\mu \in M(\bar{f})} A(\mu)\sum_{\substack{\nu \in M(\bar{f}) \\ q|\nu}} B(\nu)x^{\nu/q+\mu} \\
&= \sum_{\mu \in M(\bar{f})} A(\mu)x^{\mu}\sum_{\substack{\nu \in M(\bar{f}) \\ q|\nu}} B(\nu)x^{\nu/q} \\
&= a(x)\psi_q\left(b(x)\right).
\end{aligned}$$

□

**Proposition 2.2.13.** *Let $b$ be a nonnegative rational number. If $H(x) \in B_{\bar{f}}(b)$, then for any positive integer $l$, we have*

$$(i_q \circ \psi_q \circ H)^l = i_{q^l} \circ \psi_{q^l} \circ \prod_{j=0}^{l-1} H(x^{q^j})$$

*Proof.* This result follows from a simple induction argument. Observe that $\psi_q^l = \psi_{q^l}$

and by the lemma above, we have

$$\begin{aligned}(i_q \circ \psi_q \circ H)^2 &= i_q \circ \psi_q \circ H(x) \circ i_q \circ \psi_q \circ H(x) \\ &= i_{q^2} \circ \psi_q \circ \psi_q \circ H(x^q) H(x) \\ &= i_{q^2} \circ \psi_{q^2} \circ H(x^q) H(x)\end{aligned}$$

And similarly, if

$$(i_q \circ \psi_q \circ H)^k = i_{q^k} \circ \psi_{q^k} \circ \prod_{j=0}^{k-1} H(x^{q^j}),$$

then,

$$\begin{aligned}(i_q \circ \psi_q \circ H)^{k+1} &= i_q \circ \psi_q \circ H(x) \circ i_{q^k} \circ \psi_{q^k} \circ \prod_{j=0}^{k-1} H(x^{q^j}) \\ &= i_{q^{k+1}} \circ \psi_q \circ \psi_{q^k} \circ H(x^{q^k}) \circ \prod_{j=0}^{k-1} H(x^{q^j}) \\ &= i_{q^{k+1}} \circ \psi_{q^{k+1}} \circ \prod_{j=0}^{k} H(x^{q^j}).\end{aligned}$$

□

And finally we get the trace formula from Proposition 2.1.26 and the above results.

**Theorem 2.2.14.** *(Dwork Trace Formula) For each positive integer, $l$ we have*

$$\boxed{S_l^*(q, 1, \Theta^{(1)}, \bar{f})) = (q^l - 1)^n \operatorname{Tr}(\alpha^l)}$$

*where $\alpha = i_q \circ \psi_q \circ G_1$.*

*Proof.* From the previous proposition, we have

$$\operatorname{Tr}(\alpha^l) = \operatorname{Tr}\left( i_{q^l} \circ \psi_{q^l} \circ \prod_{j=0}^{l-1} G_1(x^{q^j}) \right)$$

Then the result follows from Proposition 2.2.11 and Proposition 2.1.26. □

We will now obtain an expression for the associated $L$-function in terms of Dwork's $\delta$-operator (with respect to $q$) defined as follows. For a rational function or Laurent series $P(t) \in K((t))$, we write $P(t)^{\delta} := \dfrac{P(t)}{P(qt)}$. Observe that the $\delta$-operator is multiplicative and an easy induction argument shows that on applying the $\delta$ operator $n$ times successively we get

$$P(t)^{\delta^n} = \prod_{j=0}^{n} P(q^j t)^{\binom{n}{j}(-1)^j} \tag{2.2.4}$$

$$= \left[\frac{P(t)}{P(qt)^{\binom{n}{1}}}\right]\left[\frac{P(q^2t)^{\binom{n}{2}}}{P(q^3t)^{\binom{n}{3}}}\right] ... P(q^n t)^{(-1)^n} \tag{2.2.5}$$

**Theorem 2.2.15.** *We have:*

*(a)*

$$L^*(q, 1, \Theta^{(1)}, \bar{f}, T) = \prod_{j=0}^{n} \left[\det(\mathbb{I} - q^j \alpha T)\right]^{(-1)^{(n-j+1)}\binom{n}{j}}$$

*(b)*

$$L^*(q, 1, \Theta^{(1)}, \bar{f}, T)^{(-1)^{(n+1)}} = \det(\mathbb{I} - \alpha T)^{\delta^n}$$

*Proof.* From the trace formula (Theorem 2.2.14) we have

$$\begin{aligned}
L^*(q, 1, \Theta^{(1)}, \bar{f}, T) &= \exp\left(\sum_{l=1}^{\infty} S_l^*(q, 1, \Theta^{(1)}, \bar{f})\frac{T^l}{l}\right) \\
&= \exp\left(\sum_{l=1}^{\infty} (q^l - 1)^n \operatorname{Tr}(\alpha^l)\frac{T^l}{l}\right) \\
&= \exp\left(\sum_{l=1}^{\infty}\sum_{j=0}^{n} \binom{n}{j} q^{lj}(-1)^{n-j} \operatorname{Tr}(\alpha^l)\frac{T^l}{l}\right) \\
&= \exp\left(\sum_{j=0}^{n}\sum_{l=1}^{\infty} \binom{n}{j} q^{lj}(-1)^{n-j} \operatorname{Tr}(\alpha^l)\frac{T^l}{l}\right) \\
&= \prod_{j=0}^{n} \exp\left(\sum_{l=1}^{\infty} \binom{n}{j} q^{lj}(-1)^{n-j} \operatorname{Tr}(\alpha^l)\frac{T^l}{l}\right)
\end{aligned}$$

$$= \prod_{j=0}^{n} \left[ \exp\left( \sum_{l=1}^{\infty} \mathrm{Tr}(\alpha^l) \frac{(q^j T)^l}{l} \right) \right]^{\binom{n}{j}(-1)^{n-j}}$$
$$= \prod_{j=0}^{n} \left[ \exp\left( -\sum_{l=1}^{\infty} \mathrm{Tr}(\alpha^l) \frac{(q^j T)^l}{l} \right) \right]^{\binom{n}{j}(-1)^{n-j+1}}$$
$$= \prod_{j=0}^{n} \left[ \det\left( \mathbb{I} - q^j \alpha T \right) \right]^{\binom{n}{j}(-1)^{n-j+1}}$$

where the last equality follows from Equation 2.2.2. Hence we have part (a). Finally, part (b) follows from Equation 2.2.4. □

We will call the operator $\psi_q$ as the *Dwork operator* or the *Dwork inverse Frobenius operator* since it is essentially a "$q$-th root" map. We will also refer to the maps $q^j\alpha$ as the *Dwork Frobenius* (or just Frobenius) maps for simplicity when there is no possible confusion. Our next goal is to realize these *Frobenius maps* as a chain map occurring on a certain complex for cohomological applications like estimating the size of the eigenvalues of these maps.

### 2.2.3 Realizing the Frobenius as a Chain Map on a Complex

Throughout the rest of this discussion, we will assume that the field $K_q = \mathbb{Q}_q(\zeta_p, \tilde{\pi})$, where $\tilde{\pi}$ is a root of an Eisenstein polynomial $t^\lambda - (1 - \zeta_p) \in \mathbb{Q}_p(\zeta_p)[t]$ for a sufficiently large positive integer $\lambda$ such that $K_q$ is sufficiently ramified over $\mathbb{Q}_q$ so that $\zeta_p \in K_q$ and all our Banach spaces defined over $K = K_q$ have convenient choices for the orthonormal bases. Also let $K_p = \mathbb{Q}_p(\zeta_p, \tilde{\pi})$. Then it is clear that $Gal(K_q/K_p)$ is isomorphic to $Gal(\mathbb{F}_q/\mathbb{F}_p)$ by an argument similar to that of Proposition 2.1.23. We will first describe another useful map $\alpha_0 : B_{\bar{f}}\left(\frac{1}{p-1}\right) \to B_{\bar{f}}\left(\frac{1}{p-1}\right)$ which satisfies $\alpha_0^a = \alpha$. This decomposition helps us realize the Frobenius maps as a chain map due to the peculiar commutativity properties of $\alpha_0$. Let $\sigma \in Gal\left(K_q/K_p\right)$ be the Frobenius generator. Then its inverse, $\sigma^{-1}$ induces a ring homomorphism $\sigma^{-1} : B_{\bar{f}}\left(\frac{p}{p-1}\right) \to B_{\bar{f}}\left(\frac{p}{p-1}\right)$ by acting on the coefficients of an element in $B_{\bar{f}}\left(\frac{p}{p-1}\right)$. We note that this induced map $\sigma^{-1}$ is *not* $K_q$-linear, although it is $K_p$-linear. We also define the $\psi_p$ linear operator

very similar to the $\psi_q$ operator defined at the beginning of this subsection (that is, $\psi_p$ is the "$p$-th root" map). Then since $F_1(x) \in B_{\bar{f}}\left(\frac{1}{p-1}, 0\right)$ we have the composite $\psi_p \circ F_1(x) : B_{\bar{f}}\left(\frac{1}{p-1}\right) \to B_{\bar{f}}\left(\frac{p}{p-1}\right)$, where the *map* $F_1(x)$ refers to "multiplication by $F_1(x)$" as before. Then we define $\alpha_0$ to be the composite

$$B_{\bar{f}}\left(\frac{1}{p-1}\right) \xrightarrow{\psi_p \circ F_1(x)} B_{\bar{f}}\left(\frac{p}{p-1}\right) \xrightarrow{\sigma^{-1}} B_{\bar{f}}\left(\frac{p}{p-1}\right) \xrightarrow{i_p} B_{\bar{f}}\left(\frac{1}{p-1}\right)$$

$\alpha_0 := i_p \circ \sigma^{-1} \circ \psi_p \circ F_1(x)$, where $i_p$ is the inclusion. Since $\sigma^{-1}$ is *not* $K_q$-linear, so is $\alpha_0$ which is only a group homomorphism. However, $\alpha_0$ is $\sigma^{-1}$-*semilinear* over $K_q$ in the following sense: For $c \in K_q$ and $\xi \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$, we have that $c\xi \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$ and it is easy to see that $\alpha_0(c\xi) = \sigma^{-1}(c)\alpha_0(\xi)$. However,

$$\alpha_0^a(c\xi) = \sigma^{-a}(c)\alpha_0^a(\xi) = c\alpha_0^a(\xi).$$

Thus, the composite $\alpha_0^a$ is $K_q$-linear even though $\alpha_0$ is not. However $\alpha_0$ is $K_p$-linear since $\sigma$ fixes $K_p$.

**Remark 2.2.16.** Note that, in fact, the induced map $\sigma^{-1}$ and the maps $\psi_{p^j}$ (where $j$ is a positive integer) can be defined on all spaces $B_{\bar{f}}(b)$ when $b$ is a nonnegative rational number. And similarly, for any $H(x) \in B_{\bar{f}}(b)$, the "multiplication by $H(x)$ map" is well defined for any nonnegative rational number, $b$. Also, for any other positive rational number $b' < b$, we have the following commutative diagrams

$$\begin{array}{ccc} B_{\bar{f}}(b) & \xrightarrow{\sigma^{-1}} & B_{\bar{f}}(b) \\ \downarrow i & & \downarrow i \\ B_{\bar{f}}(b') & \xrightarrow{\sigma^{-1}} & B_{\bar{f}}(b') \end{array} \qquad \begin{array}{ccc} B_{\bar{f}}(b) & \xrightarrow{H(x)} & B_{\bar{f}}(b) \\ \downarrow i & & \downarrow i \\ B_{\bar{f}}(b') & \xrightarrow{H(x)} & B_{\bar{f}}(b') \end{array} \qquad \begin{array}{ccc} B_{\bar{f}}(b) & \xrightarrow{\psi_{p^j}} & B_{\bar{f}}\left(p^j b\right) \\ \downarrow i & & \downarrow i \\ B_{\bar{f}}(b') & \xrightarrow{\psi_{p^j}} & B_{\bar{f}}\left(p^j b'\right) \end{array}$$

where $i$ denotes the inclusion maps. Hence, we may ignore specifying the exact domain of these maps which is usually inferred from the context when performing some computations. We also observe that $\psi_p^j = \psi_{p^j}$ for any positive integer $j$, analogous to what we had for $\psi_q$.

**Proposition 2.2.17.** *Let $H(x) \in B_{\bar{f}}(b)$ for some $b \in \mathbb{Q}_{\geq 0}$ such that $b \leq \frac{1}{p-1}$. Then*

*(a)*

$$F(x) \circ \sigma^{-1}(H(x)) = \sigma^{-1} \circ F^{\sigma}(x)(H(x))$$

*(b)*

$$\psi_p \circ \sigma^{-1}(H(x)) = \sigma^{-1} \circ \psi_p(H(x))$$

*(c) If* $L(x) \in B_{\bar{f}}\left(\frac{p}{q(p-1)}\right)$, *then* $\alpha_0^a(L(x)) = \alpha(L(x))$.

*Proof.* Statements $(a)$ and $(b)$ are trivial. Statement $(c)$ follows from statements $(a)$ and $(b)$ and from an analogue of Lemma 2.2.12 for the $\psi_p$ map. That is, we have for $A(x), B(x) \in B_{\bar{f}}(b)$,

$$A(x)\psi_p[B(x)] = \psi_p[A(x^p)B(x)], \text{ that is, } A(x) \circ \psi_p[B(x)] = \psi_p \circ A(x^p)[B(x)]$$

so that we have

$$\begin{aligned}
\alpha_0^a(L(x)) &= (i_p \circ \sigma^{-1} \circ \psi_p \circ F(x))^a(L(x)) \\
&= (\sigma^{-1} \circ \psi_p \circ F(x))^a(L(x)) \\
&= (\sigma^{-1} \circ \psi_p \circ F(x)) \circ (\sigma^{-1} \circ \psi_p \circ F(x)) \circ ... \circ (\sigma^{-1} \circ \psi_p \circ F(x))(L(x)) \\
&= \left(\sigma^{-a} \circ (\psi_p \circ F^{\sigma^{a-1}}(x)) \circ (\psi_p \circ F^{\sigma^{a-2}}(x)) \circ ... \circ (\psi_p \circ F^{\sigma}(x)) \circ (\psi_p \circ F(x))\right) \\
&\qquad\qquad (L(x)) \\
&= \left(\sigma^{-a} \circ \psi_p^a \circ F^{\sigma^{a-1}}(x^{p^{a-1}}) F^{\sigma^{a-2}}(x^{p^{a-2}}) ... F^{\sigma}(x^p) F(x)\right)(L(x)) \\
&= (\psi_{p^a} \circ G_1(x))(L(x)) \\
&= (i_q \circ \psi_q \circ G_1(x))(L(x)) \\
&= \alpha(L(x))
\end{aligned}$$

where the omissions of the inclusion maps $i_p$ and our slight abuses in notations make sense by Remark 2.2.16 above. □

Now, our goal is to construct a certain complex on which the Frobenius maps, $q^j\alpha$ act as a chain map. In order to construct such a complex, we need a good differential operator which acts as boundary maps on the complex. It turns out that the operator

$x_i \frac{\partial}{\partial x_i}$ (defined in the usual way) has *good* commutativity properties with the maps $\psi_p$ and $\psi_q$ and hence we may construct a certain Koszul complex whose boundary maps are derived from these operators.

**Lemma 2.2.18.** *Let $b$ be a nonnegative rational number and $j$ a positive integer and $i \in \{1, 2, ..., n\}$. Then on $B_{\bar{f}}(b)$, we have*

*(a)*

$$p^j x_i \frac{\partial}{\partial x_i} \circ \psi_{p^j} = \psi_{p^j} \circ x_i \frac{\partial}{\partial x_i}$$

*(b)*

$$\sigma^{-1} \circ x_i \frac{\partial}{\partial x_i} = x_i \frac{\partial}{\partial x_i} \circ \sigma^{-1}$$

*Proof.* It suffices to prove statement $(a)$ for a monomial $x^\nu \in B_{\bar{f}}(b)$. If $p^j | \nu$, then we have

$$p^j x_i \frac{\partial}{\partial x_i} \circ \psi_{p^j}(x^\nu) = p^j x_i \frac{\partial}{\partial x_i}(x^{p^{-j}\nu}) = \nu_i x^{p^{-j}\nu} = \psi_{p^j}(\nu_i x^\nu) = \psi_{p^j} \circ x_i \frac{\partial}{\partial x_i}(x^\nu)$$

and the result is trivial when $p^j \nmid \nu$. Statement $(b)$ follows from the fact that $\sigma^{-1}$ acts trivially on rational integers occurring as coefficients upon differentiation. □

**Lemma 2.2.19.** *(Twist Lemma) Suppose that $F(x)$ can be written as $F(x) = \dfrac{H(x)}{H^\sigma(x^p)}$ for some invertible $H(x) \in B_{\bar{f}}(b, 0)$ for some rational number $b$ such that $0 \leq b \leq \frac{1}{p-1}$. Then*

*(a)*

$$G_1(x) = \frac{H(x)}{H(x^q)}$$

*(b) On $B_{\bar{f}}(\frac{1}{p-1})$,*

$$\psi_p \circ F(x) = \frac{1}{H^\sigma(x)} \circ \psi_p \circ H(x)$$

*And similarly, on $B_{\bar{f}}(\frac{p}{q(p-1)})$,*

$$\psi_q \circ G_1(x) = \frac{1}{H(x)} \circ \psi_q \circ H(x)$$

*(Note that the multiplication by $H(\mathbf{x})$ acts on a much larger space, $B_{\bar{f}}(b)$ but the compositions are stable on the spaces indicated.)*

*(c) On* $B_{\bar{f}}(\frac{1}{p-1})$,

$$\sigma^{-1} \circ \psi_p \circ F(x) = \frac{1}{H(x)} \circ \sigma^{-1} \circ \psi_p \circ H(x)$$

*Proof.* Statement $(a)$ follows from the definition of $G_1(x)$ and from the fact that $\sigma^{-1}$ is a ring homomorphism on $B_{\bar{f}}(0)$. Next we observe that $\frac{1}{H(x)} \in B_{\bar{f}}(0,0) \subset B_{\bar{f}}(0)$ whenever $H(x) \in B_{\bar{f}}(0,0)$ and is invertible. Statement $(b)$ follows from Lemma 2.2.12 and its analogue for $\psi_p$. To prove statement $(c)$, observe again that $\sigma^{-1}$ is a ring homomorphism on $B_{\bar{f}}(0)$, and hence

$$\sigma^{-1} \circ \frac{1}{H^\sigma(x)} = \frac{1}{H(x)} \circ \sigma^{-1}.$$

And therefore,

$$\begin{aligned}
\sigma^{-1} \circ \psi_p \circ F_1(x) &= \sigma^{-1} \circ \psi_p \circ \frac{H(x)}{H^\sigma(x^p)} \\
&= \sigma^{-1} \circ \psi_p \circ \frac{1}{H^\sigma(x^p)} \circ H(x) \\
&= \sigma^{-1} \circ \frac{1}{H^\sigma(x)} \circ \psi_p \circ H(x) \\
&= \frac{1}{H(x)} \circ \sigma^{-1} \circ \psi_p \circ H(x)
\end{aligned}$$

where the third inequality follows from the analogue of Lemma 2.2.12 for $\psi_p$. □

The above commutativity properties motivate us to define the linear operators $L_i : B_{\bar{f}}\left(\frac{1}{p-1}\right) \to B_{\bar{f}}\left(\frac{1}{p-1}\right)$ given by

$$L_i := \frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)$$

for $i = 1, 2, ..., n$, whenever we are able to write $F(x) = \frac{H(x)}{H^\sigma(x^p)}$. And in this case the operators $L_i$ enjoy very good commutativity properties and are useful in the construction of the complex. The following proposition shows that this is indeed the case.

**Proposition 2.2.20.** *The splitting function,* $\theta_1(t)$ *can be written as* $\theta_1(t) = \frac{\phi(t)}{\phi(t^p)}$

*in terms of another convergent power series,* $\phi(t) \in \mathbb{Q}_q(\zeta_p)[[t]]$ *which converges for* $\operatorname{ord}_p t > 0$.

*Proof.* Let us define $\phi(t) := \prod_{j=0}^{\infty} \theta_1(t^{p^j})$. Then this infinite product converges in the formal topology (topology of coefficientwise convergence) [Dwo62] of $\mathbb{C}_p[[t]]$ and we have

$$\begin{aligned}\frac{\phi(t)}{\phi(t^p)} &= \frac{\prod_{j=0}^{\infty} \theta_1(t^{p^j})}{\prod_{j=1}^{\infty} \theta_1(t^{p^j})} \\ &= \prod_{j=0}^{\infty} \frac{\theta_1(t^{p^j})}{\theta_1(t^{p^{j+1}})} \\ &= \theta_1(t)\end{aligned}$$

due to successive cancellations. It remains to show the convergence of $\phi(t)$. Recall that $\theta_1(t) = \exp\left[\sum_{j=0}^{\infty} \frac{(\gamma_1 t)^{p^j}}{p^j}\right]$ where $\gamma_1$ is a zero of $S(t) := \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$ such that $\operatorname{ord}_p \gamma_1 = \frac{1}{p-1}$. Then, we may write

$$\begin{aligned}\phi(t) &= \prod_{i=0}^{\infty} \theta_1(t^{p^i}) \\ &= \prod_{i=0}^{\infty} \exp\left[\sum_{j=0}^{\infty} \frac{(\gamma_1 t^{p^i})^{p^j}}{p^j}\right] \\ &= \exp\left[\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} \frac{(\gamma_1 t^{p^i})^{p^j}}{p^j}\right] \\ &= \exp\left(\sum_{i=0}^{\infty} \beta_i t^{p^i}\right)\end{aligned}$$

where the coefficients $\beta_i$ are given by $\beta_i = \sum_{j=0}^{i} \frac{\gamma_1^{p^j}}{p^j}$. Now, since $S(\gamma_1) = \sum_{j=0}^{\infty} \frac{\gamma_1^{p^j}}{p^j} = 0$, we have that $\beta_i = -\sum_{j=i+1}^{\infty} \frac{\gamma_1^{p^j}}{p^j}$ and therefore,

$$\begin{aligned}\operatorname{ord}_p(\beta_i) &= \operatorname{ord}_p\left(-\sum_{j=i+1}^{\infty} \frac{\gamma_1^{p^j}}{p^j}\right) \\ &\geq \inf_{j \geq i+1} \operatorname{ord}_p\left(\frac{\gamma_1^{p^j}}{p^j}\right)\end{aligned}$$

$$= \inf_{j \geq i+1} \left[ \frac{p^j}{p-1} - j \right]$$
$$= \frac{p^{i+1}}{p-1} - (i+1)$$

where the last equality holds for $i \geq 0$ due to the fact that the real valued function $g(y) = \frac{p^y}{p-1} - y$ is increasing for $y \geq 1$. And therefore, $\frac{p^i}{p-1} - i$ tends to $\infty$ as $i$ tends to $\infty$. Also clearly, when $\mathrm{ord}_p\, t > 0$,

$$\mathrm{ord}_p \left( \sum_{i=0}^{\infty} \beta_i t^{p^i} \right) > \inf_{i \geq 0} (\mathrm{ord}_p(\beta_i))$$
$$\geq \frac{p}{p-1} - 1$$
$$= \frac{1}{p-1}.$$

Hence, $\phi(t) = \exp\left( \sum_{i=0}^{\infty} \beta_i t^{p^i} \right)$ converges for $\mathrm{ord}_p\, t > 0$. □

**Corollary 2.2.21.** *There exists an invertible power series $H(x) \in B_{\bar{f}}(0,0)$ such that $F(x) = \dfrac{H(x)}{H^\sigma(x^p)}$.*

*Proof.* Recall that $F(x) = \prod_{\mu \in Supp(\bar{f})} \theta_1(a_\mu x^\mu)$ where the $a_\mu$ are the Teichmüller lifts of the coefficients $\bar{a}_\mu$ of the Laurent polynomial, $\bar{f}(\bar{x})$. We may set $H(x) = \prod_{\mu \in Supp(\bar{f})} \phi(a_\mu x^\mu)$, where $\phi(t)$ is the series in the previous proposition. Then since $\sigma(a_\mu) = a_\mu^p$ and $\theta_1(t) = \phi(t)/\phi(t^p)$, we have that $F(x) = \dfrac{H(x)}{H^\sigma(x^p)}$. And it is easily seen that $H(x) \in B_{\bar{f}}(0,0)$ (for instance, by an analogue of Lemma 2.2.7). □

Hence, indeed we can write $F(x) = \dfrac{H(x)}{H^\sigma(x^p)}$ and therefore we may define the linear operators

$$L_i = \frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)$$

on the space $B_{\bar{f}}\left(\dfrac{1}{p-1}\right)$ for $i = 1, 2, ..., n$.

**Remark 2.2.22.** It is to be observed carefully that the operators $L_i$ are stable on the space $B_{\bar{f}}\left(\dfrac{1}{p-1}\right)$ even though the individual map "multiplication by $H(x)$" (defined on a bigger space, $B_{\bar{f}}(0)$) need not be stable on the subspace $B_{\bar{f}}\left(\dfrac{1}{p-1}\right)$. Let $\phi(t)$ be the

power series defined in Proposition 4.2.5. Writing $\phi(t) = \exp\beta(t)$ where $\beta(t) = \sum_{j=0}^{\infty} \beta_j t^{p^j}$ as in Proposition 4.2.5 with the coefficients $\beta_j$ satisfying

$$\operatorname{ord}_p \beta_j \geq \frac{p^{j+1}}{p-1} - (j+1)$$

we observe that

$$\frac{1}{\exp\beta(t)} \circ t\frac{\partial}{\partial t} \circ \exp\beta(t) = t\frac{\partial}{\partial t} + t\frac{\partial \beta}{\partial t}$$

by the product rule and the chain rule of the derivative operator. In the same way, for $H(x) = \prod_{\mu \in Supp(\bar{f})} \phi(a_\mu x^\mu)$, we have

$$\begin{aligned}
L_i = \frac{1}{H(x)} \circ x_i\frac{\partial}{\partial x_i} \circ H(x) &= \frac{1}{\prod_{\mu \in Supp(\bar{f})} \phi(a_\mu x^\mu)} \circ x_i\frac{\partial}{\partial x_i} \circ \prod_{\mu \in Supp(\bar{f})} \phi(a_\mu x^\mu) \\
&= \frac{1}{\prod_{\mu \in Supp(\bar{f})} \exp\beta(a_\mu x^\mu)} \circ x_i\frac{\partial}{\partial x_i} \circ \prod_{\mu \in Supp(\bar{f})} \exp\beta(a_\mu x^\mu) \\
&= \frac{1}{\exp\left(\sum_{\mu \in Supp(\bar{f})} \beta(a_\mu x^\mu)\right)} \circ x_i\frac{\partial}{\partial x_i} \circ \exp\left(\sum_{\mu \in Supp(\bar{f})} \beta(a_\mu x^\mu)\right) \\
&= \frac{1}{\exp\tilde{H}(x)} \circ x_i\frac{\partial}{\partial x_i} \circ \exp\tilde{H}(x) \\
&= x_i\frac{\partial}{\partial x_i} + x_i\frac{\partial \tilde{H}}{\partial x_i}
\end{aligned}$$

where $\tilde{H}(x) = \sum_{\mu \in Supp(\bar{f})} \beta(a_\mu x^\mu)$. Thus, in order to show that $L_i$ is stable on $B_{\bar{f}}\left(\frac{1}{p-1}\right)$, it suffices to show that the power series $x_i\frac{\partial \tilde{H}}{\partial x_i} \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$ since the operator $x_i\frac{\partial}{\partial x_i}$ is automatically stable on $B_{\bar{f}}\left(\frac{1}{p-1}\right)$ as the derivative only introduces integer coefficients. In fact, we can show something stronger.

**Proposition 2.2.23.** *Let $\tilde{H}(x)$ be the be the power series as defined above. Then for each $i = 1, 2, ..., n$,*

$$x_i\frac{\partial \tilde{H}}{\partial x_i} \in B_{\bar{f}}\left(\frac{p}{p-1}, -1\right) \subset B_{\bar{f}}\left(\frac{1}{p-1}\right)$$

*Proof.* We have,

$$\begin{aligned} x_i\frac{\partial \tilde{H}}{\partial x_i} &= x_i\frac{\partial}{\partial x_i}\left(\sum_{\mu\in Supp(\bar{f})}\sum_{j=0}^{\infty}\beta_j a_\mu^{p^j}x^{\mu p^j}\right) \\ &= x_i\frac{\partial}{\partial x_i}\left(\sum_{j=0}^{\infty}\beta_j\sum_{\mu\in Supp(\bar{f})}a_\mu^{p^j}x^{\mu p^j}\right) \\ &= \sum_{j=0}^{\infty}\beta_j x_i\frac{\partial}{\partial x_i}\left(\sum_{\mu\in Supp(\bar{f})}a_\mu^{p^j}x^{\mu p^j}\right) \\ &= \sum_{j=0}^{\infty}\beta_j\left(\sum_{\mu\in Supp(\bar{f})}a_\mu^{p^j}p^j x^{\mu p^j}\right) \end{aligned}$$

Hence we may write $x_i\dfrac{\partial \tilde{H}}{\partial x_i} = \sum\limits_{\nu\in M(\bar{f})} C(\nu)x^\nu$ with coefficients, $C(\nu)$ given by

$$C(\nu) = \sum \beta_j a_\mu^{p^j}p^j$$

where the sum is over the set $S = \{(\mu, j) : \mu \in Supp(\bar{f}), j \in \mathbb{Z}_{\geq 0}, \mu p^j = \nu\}$. Then we have

$$\begin{aligned} \operatorname{ord}_p C(\nu) &\geq \inf_{(\mu,j)\in S}(\operatorname{ord}_p \beta_j + j) \\ &\geq \inf_{(\mu,j)\in S}\left(\frac{p^{j+1}}{p-1} - (j+1) + j\right) \\ &= \frac{p}{p-1}\left(\inf_{(\mu,j)\in S} p^j\right) - 1 \\ &\geq \frac{p}{p-1}\left(\inf\left\{\sum_{\mu\in Supp(\bar{f})} r_\mu : \sum_{\mu\in Supp(\bar{f})} r_\mu\mu = \nu, r_\mu \in \mathbb{Q}_{\geq 0}\right\}\right) - 1 \\ &= \frac{p}{p-1}w(\nu) - 1 \end{aligned}$$

□

**Proposition 2.2.24.** *On* $B_{\bar{f}}\left(\dfrac{1}{p-1}\right)$, $pL_i \circ \alpha_0 = \alpha_0 \circ L_i$.

*Proof.*

$$\begin{aligned}
pL_i \circ \alpha_0 &= p\left[\frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)\right] \circ \left[i_p \circ \sigma^{-1} \circ \psi_p \circ \frac{H(x)}{H^\sigma(x^p)}\right] \\
&= p\left[\frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)\right] \circ \left[i_p \circ \frac{1}{H(x)} \circ \sigma^{-1} \circ \psi_p \circ H(x)\right] \\
&= p\left[\frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ i_p \circ \sigma^{-1} \circ \psi_p \circ H(x)\right] \\
&= p\left[\frac{1}{H(x)} \circ i_p \circ \sigma^{-1} \circ x_i \frac{\partial}{\partial x_i} \circ \psi_p \circ H(x)\right] \\
&= \left[\frac{1}{H(x)} \circ i_p \circ \sigma^{-1} \circ p x_i \frac{\partial}{\partial x_i} \circ \psi_p \circ H(x)\right] \\
&= \left[\frac{1}{H(x)} \circ i_p \circ \sigma^{-1} \circ \psi_p \circ x_i \frac{\partial}{\partial x_i} \circ H(x)\right] \\
&= \left[\frac{1}{H(x)} \circ i_p \circ \sigma^{-1} \circ \psi_p \circ H(x) \circ \frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)\right] \\
&= \left[i_p \circ \frac{1}{H(x)} \circ \sigma^{-1} \circ \psi_p \circ H(x)\right] \circ \left[\frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)\right] \\
&= \left[i_p \circ \sigma^{-1} \circ \psi_p \circ \frac{H(x)}{H^\sigma(x^p)}\right] \circ \left[\frac{1}{H(x)} \circ x_i \frac{\partial}{\partial x_i} \circ H(x)\right] \\
&= \alpha_0 \circ L_i
\end{aligned}$$

where the chain of equalities follow from the commutativity properties proved above: Proposition 2.2.17, Lemma 2.2.18 and Lemma 2.2.19. □

**Corollary 2.2.25.** *On* $B_{\bar{f}}\left(\frac{1}{p-1}\right)$, $qL_i \circ \alpha = \alpha \circ L_i$.

*Proof.* This result is a trivial consequence of Proposition 2.2.24 and statement $(c)$ in Proposition 2.2.17. □

We may now construct the Koszul complex on which the Frobenius maps $q^j\alpha$ act as a chain map. Let $M = B_{\bar{f}}\left(\frac{1}{p-1}\right)$. Then the linear operators $L_i : M \to M$ commute with eact other, that is, $L_iL_j = L_jL_i$ for all $i, j \in \{1, 2, ..., n\}$ since the mixed partial derivatives are equal independent of the order of differentiation. Let $S$ be the ring $\mathbb{Z}[L_1, L_2, ..., L_n]$. Then $M$ has a natural $S$-module structure under the action $L_i.m = L_i(m)$ for $m \in M$. Let $\mathbf{L} = (L_1, L_2, ..., L_n)$ and let $K^\bullet(\mathbf{L}, S)$ denote the Koszul cochain complex on $S$ with respect to $\mathbf{L}$. Let $K^\bullet(\mathbf{L}, M) := K^\bullet(\mathbf{L}, S) \otimes_S M$. We will construct this complex by first constructing $K^\bullet(\mathbf{L}, R)$ as follows. Set $K_S^i = 0$ for $i \in \mathbb{Z} - \{0, 1, 2, ..., n\}$.

Then set $K_S^0 = S$ and $K_S^1 = S^n$. Set $K_S^i = \bigwedge^i(K_S^1)$, the $i$-th exterior power of the free $S$-module, $K_S^1$ of rank $n$, for $i = 2, 3, ..., n$. Let $\{e_1, e_2, ..., e_n\}$ be a basis for $K_S^1$. Then it is clear that $K_S^i$ is a free $S$-module of rank $\binom{n}{i}$ for $i = 2, 3, ..., n$ and they are given by

$$K_S^i = \bigoplus_{1 \leq j_1 < j_2 < ... < j_i \leq n} S(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

And the boundary maps $\partial_S^i : K_S^i \to K_S^{i+1}$ are given by

$$\partial_S^i(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) = \sum_{k=1}^{n} L_k(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

for $i = 1, 2, ..., n-1$ and $\partial_S^0 : K_S^0 \to K_S^1$ is given by $\partial_S^0(1) = \sum_{k=1}^{n} L_k e_k$.

Tensoring the complex $K^\bullet(\mathbf{L}, S)$ with $M$ over $S$, we get the complex $K^\bullet(\mathbf{L}, M)$ composed of free $S$-modules, $K^i$ given by $K^i = 0$ for $i \in \mathbb{Z} - \{0, 1, 2, ..., n\}$ and $K^1 = M$ and

$$K^i = \bigoplus_{1 \leq j_1 < j_2 < ... < j_i \leq n} M(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

for $i = 2, 3, ..., n$ with the boundary maps $\partial^i : K^i \to K^{i+1}$ given by

$$\partial^i(me_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) = \sum_{k=1}^{n} L_k(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

for $i = 1, 2, ..., n-1$ and $\partial^0 : K^0 \to K^1$ is given by $\partial^0(m) = \sum_{k=1}^{n} L_k(m)e_k$. It is easily seen that $\partial_S \partial_S = 0$ and $\partial\partial = 0$.

We may now define the $S$-linear map $\mathbf{Frob} : K^\bullet(\mathbf{L}, M) \to K^\bullet(\mathbf{L}, M)$ as follows. For $i = 1, 2, ..., n$, define $\mathbf{Frob}|^i : K^i \to K^i$ by

$$\mathbf{Frob}|^i = \bigoplus_{1 \leq j_1 < j_2 < ... < j_i \leq n} q^{n-i}\alpha(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

and define $\mathbf{Frob}|^0 : K^0 \to K^0$ by $\mathbf{Frob}|^0 = q^n\alpha$.

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & K^0 \cong M & \xrightarrow{\partial^0} & K^1 \cong M^{\binom{n}{1}} & \xrightarrow{\partial^1} & K^2 \cong M^{\binom{n}{2}} & \xrightarrow{\partial^2} & \ldots & \xrightarrow{\partial^{n-1}} & K^n \cong M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle q^n\alpha} & & \downarrow{\scriptstyle \oplus_i q^{n-1}\alpha(e_i)} & & \downarrow{\scriptstyle \oplus_{i<j} q^{n-2}\alpha(e_i\wedge e_j)} & & & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & K^0 & \xrightarrow{\partial^0} & K^1 & \xrightarrow{\partial^1} & K^2 & \xrightarrow{\partial^2} & \ldots & \xrightarrow{\partial^{n-1}} & K^n & \longrightarrow & 0
\end{array}$$

Figure 2.1: Action of the Dwork Frobenius on the Dwork Complex: $r = 1$ case

**Proposition 2.2.26.** *The map* **Frob** *defined above is a chain map on the complex,* $K^\bullet(\mathbf{L}, M)$.

*Proof.* For each $i = 0, 1, 2, ..., n-1$ and $1 \le j_1 < j_2 < ... < j_i \le n$ and for $m \in M$, we have

$$\begin{aligned}
\partial^i \circ \mathbf{Frob}|^i \left[m(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})\right] &= \partial^i \left[q^{n-i}\alpha(m)(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})\right] \\
&= \sum_{k=1}^{n} L_k \left(q^{n-i}\alpha(m)\right)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \sum_{k=1}^{n} q^{n-i-1}(qL_k \circ \alpha)(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \sum_{k=1}^{n} q^{n-i-1}(\alpha \circ L_k)(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \sum_{k=1}^{n} (q^{n-(i+1)}\alpha) \circ L_k(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= q^{n-(i+1)}\alpha \circ \sum_{k=1}^{n} L_k(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \mathbf{Frob}|^{i+1} \circ \partial^i \left[m(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})\right]
\end{aligned}$$

where the crucial fourth equality follows from Corollary 2.2.25. □

**Theorem 2.2.27.**

$$L^*(q, 1, \Theta^{(1)}, \bar{f}, T)^{(-1)^{(n+1)}} = \prod_{j=0}^{n} \left[\det(\mathbb{I} - T\mathbf{Frob}|^{n-j})\right]^{(-1)^j}$$

*Proof.* The result follows from Theorem 2.2.15 and from the observation that

$$\left[\det(\mathbb{I} - q^j\alpha T)\right]^{\binom{n}{j}} = \det(\mathbb{I} - T\mathbf{Frob}|^{n-j})$$

for $j = 0, 1, ..., n$. $\square$

The complex constructed above is called the *Dwork complex* and its cohomology is called the *Dwork cohomology*. It is natural to ask if there is an equivalent statement of the above theoerem on cohomology. That is, when we write

$$\mathbf{Frob}|^{n-j} \text{ as } \mathbf{Frob}|^{n-j}_{K^{n-j}}$$

to emphasize that the map $\mathbf{Frob}|^{n-j}$ acts on the infinite dimensional Banach space, $K^{n-j}$, and when we write

$$H(\mathbf{Frob})|^{n-j}_{H^{n-j}(K^\bullet)}$$

to denote the corresponding map on the cohomology, do we have

$$\boxed{\det(\mathbb{I} - T\mathbf{Frob}|^{n-j}_{K^{n-j}}) = \det(\mathbb{I} - TH(\mathbf{Frob})|^{n-j}_{H^{n-j}(K^\bullet)})}?$$

We note from ([Ser62]: Proposition 2) that if the images of the boundary maps $\partial^i$ in the complex are *closed* subspaces, then the maps $H(\mathbf{Frob})|^{n-j}_{H^{n-j}(K^\bullet)}$ are well defined and the above equation holds. However, it is not always the case that the images are closed. To rectify this difficulty, Monsky [Mon70] instead defines a larger class of operators called *nuclear maps* that generalize completely continuous operators. Nuclear maps are trace-class operators that have well-defined traces and Fredholm determinants. Completely continuous operators are special cases of nuclear maps whose traces can be realized in terms of orthonormal bases, and for which Serre's result applies. However, Monsky's theorem ([Mon70]: Theorem 6.11) shows that the $\mathbf{Frob}|^{n-j}_{K^{n-j}}$ being nuclear on $K^{n-j}$ imply that the $H(\mathbf{Frob})|^{n-j}_{H^{n-j}(K^\bullet)}$ are nuclear on $H^{n-j}(K^\bullet)$ as well. And thus, the boxed equation above holds true. Hence, we have

**Theorem 2.2.28.**

$$\boxed{L^*(q, 1, \Theta^{(1)}, \bar{f}, T)^{(-1)^{(n+1)}} = \prod_{j=0}^{n} \left[\det(\mathbb{I} - TH(\mathbf{Frob})|^{n-j}_{H^{n-j}(K^\bullet)})\right]^{(-1)^j}}.$$

# Chapter 3

# A Generalized Dwork Trace Formula

The goal of this chapter is to prove an analogue of Corollary 2.2.8 for the exponential sums we defined in Section 2.1.3 of Chapter 2, for the case when $r > 1$. This depends on evaluating the character values inside the exponential sums $S_l^*$ using the $p$-adic interpolation of characters by Theorem 2.1.18 [Bla03] for the case when $r > 1$ and obtaining estimates for the growth of the coefficients of the associated power series analogous to the series $F(x)$ that we had in the case when $r = 1$ in Chapter 2. That is, we express

$$\Theta^{(r)} \circ \tau(q, l, r)(\bar{f}(\bar{\mathbf{x}})) = \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} F_{i,j}(\mathbf{x})$$

for some power series $F_{i,j}(\mathbf{x})$ in $nr$ variables and then obtain estimates for the $p$-adic size of the coefficients of the power series $F_{0,0}(\mathbf{x})$ in terms of an appropriate weight function and prove the analogous results Proposition 3.2.25 and Corollary 3.2.30 for the case when $r > 1$. Having established these results, a generalized Dwork trace formula is proven easily by following the arguments in Chapter 2 (please see the beginning of Chapter 4). Note that the analogue of Proposition 2.1.26 is easily proven (by the same argument) for $r > 1$ (please see the beginning of Chapter 4).

For a better exposition of the results, to clarify the development of the cumbersome

notation and to identify and clarify technical issues, we will first consider the single variable case and further specializing to the cases when $r = 2$ and $r = 3$. We will then generalize the results to the multivariable case for all $r > 1$.

## 3.1 The Single Variable Case

Let $r$ be a positive integer and let $\bar{f}(\bar{x}) \in (\mathbb{Z}_q/p^r\mathbb{Z}_q)[\bar{x}]$ be a polynomial in one variable of degree $m$ written out as

$$\bar{f}(\bar{x}) = \bar{a}_m\bar{x}^m + \bar{a}_{m-1}\bar{x}^{m-1} + ... + \bar{a}_1\bar{x}.$$

We recall that our goal is to obtain a trace formula for the exponential sums,

$$S_l^* = S_l^*(q, r, \Theta^{(r)}, \bar{f}) = \sum \Theta^{(r)} \circ \tau(q, l, r)(\bar{f}(\bar{x})) \tag{3.1.1}$$

as defined in Chapter 2 earlier for the case when $r = 1$ and obtain a similar $p$-adic analytic expression for the associated $L$-function. We also recall that the sum runs over those $\bar{x} \in \left(\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}\right)^n$ with the $\bar{x}$ written as $\bar{x} = \sum_{k=0}^{r-1} x_k p^k$ in terms of Teichmüller digits $x_k$ satisfying $x_k^{q^l-1} = 1$. We also let the coefficients $\bar{a}_\mu \in \mathbb{Z}_q/p^r\mathbb{Z}_q$ written as

$$\bar{a}_\mu = \sum_{j=0}^{r-1} a_{\mu,j}p^j$$

in terms of Teichmüller digits $a_{\mu,j}$ satisfying $a_{\mu,j}^q = a_{\mu,j}$ for $\mu = 1, 2, ..., m$.

Now, note that in the case when $\bar{x} \in \mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ where $l$ is a positive integer, we may write $\bar{x}$ as

$$\bar{x} = \sum_{j=0}^{r-1} x_j p^j$$

in terms of Teichmüller digits $x_j$ satisfying $x_j^{q^l} = x_j$. Then consider a monomial $\bar{x}^\mu$ for a

nonnegative integer exponent $\mu$. Writing $\bar{x}$ as above when evaluating the character sum 3.1.1, we are ultimately interested in finding the monomials of the form $(\prod_j x_j^{\nu_j})p^{\nu(p)}$ occurring in the multinomial expansion of

$$\bar{x}^{\mu} = (x_0 + x_1 p + ... + x_{r-1}p^{r-1})^{\mu}.$$

And note that we are only interested in those monomials for which the exponent of $p$, $\nu(p)$ is less than $r$. The following lemmas are useful in determining the monomials of interest.

**Lemma 3.1.1.** *Let $R$ be an arbitrary commutative ring with unity and of characteristic $p^r$. Let $y = (y_0 + y_1 p + ... + y_{r-1}p^{r-1}) \in R[y_0, y_1, ..., y_{r-1}]$. Then*

*(a) There exists a unique $R$-linear derivation, $D : R[y_0, y_1, ..., y_{r-1}] \to R[y_0, y_1, ..., y_{r-1}]$ defined by $D(y_i) = y_{i+1}$ for $i = 0, 1, ..., r-2$ and $D(y_{r-1}) = 0$.*

*(b) For a given positive integer $m$, the monomials occurring in the multinomial expansion of $y^m$ satisfy the following:*

*If none of the multinomial coefficients are divisible by $p$, then*

*(i) The monomials occuring as coefficients of $p$ are those occurring in $D(y_0^m)$.*

*(ii) Similarly, for each $i = 1, 2, ..., r-2$, the monomials occuring as coefficients of $p^{i+1}$ are precisely those occurring in the image under $D$ of those monomials occurring as coefficients of $p^i$.*

*Proof.*

(a) Suppose there exists such a derivation, $D$. Clearly $D(1) = 0$. An easy induction shows that $D(y_i^m) = m y_i^{m-1} y_{i+1}$ for any positive integer $m$ and for $i = 0, 1, ..., r-2$. And hence, for a given monomial $\prod_{i=0}^{r-1} y_i^{m_i}$, we can compute $D\left(\prod_{i=0}^{r-1} y_i^{m_i}\right)$ uniquely using the *Leibniz* rule. Existence and uniqueness of $D$ follows.

(b) Consider the $r \times m$ matrix

$$\begin{pmatrix} y_0 & y_0 & \cdots & y_0 \\ y_1 p & y_1 p & \cdots & y_1 p \\ \vdots & \vdots & \ddots & \vdots \\ y_{r-1} p^{r-1} & y_{r-1} p^{r-1} & \cdots & y_{r-1} p^{r-1} \end{pmatrix}.$$

A monomial occurring in the multinomial expansion of $y^m$ corresponds to a choice of $m$ entries in the matrix one from each column such that the power of $p$ in the product of the chosen entries is less than $r$. The operator $D$ acts on this monomial precisely by replacing exactly one entry in the chosen product by the corresponding entry (excluding the $p$-power) in the *next* row and then summing over all such replaced products. (And if an entry is already in the last row, then we simply set the corresponding replaced product to be equal to zero).

For example, the monomial, $y_0^{m-2} y_1^2$ occurring as a coeffifient of $p^2$ in the expansion of $y^m$ may be realized as the choice $v = (y_1 p, y_0, y_1 p, y_0, y_0, ..., y_0)$ where the $i$-th element of the vector $v$ is chosen from the $i$-th column of the matrix. Then

$$D(y_0^{m-2} y_1^2) = (m-2) y_0^{(m-3)} y_1^3 + 2 y_0^{m-2} y_1 y_2$$

corresponds to the collection $\{v^{(j)}\}$ of $m$ vectors such that each of the $v^{(j)}$ differs from $v$ in exactly one coordinate where the entry in $v$ is replaced by the corresponding entry (excluding the $p$-power) in the next row of the matrix. And this is precisely how we obtain the monomials occurring as coefficients of $p^i$ in the multinomial expansion of $y^m$.

□

**Remark 3.1.2.** Note that there will be more complications in finding the monomials occurring as coefficients of $p^i$ in the multinomial expansion of $y^m$ in the above lemma if the multinomial coefficients are divisible by $p$. However, since we are interested in the $p$-adic growth of the coefficients of the power series analogous to $G_1(x)$ obtained from sums of character values of $\bar{f}(\bar{x})$, the above lemma is still useful to provide reasonable bounds

for the $p$-adic size of the coefficients. The $p$-divisibility of the multinomial coefficients only help rather than hurt us.

The following lemma is a well-known fact in combinatorics.

**Lemma 3.1.3.**

*Let $n$ be a positive integer. Then the number of nonnegative integer solutions to the equation*

$$\sum_{j=1}^{n} jb_j = n$$

*is the number of partitions of $n$.*

*Proof.*

We have a bijection between the set of all partitions of $n$ and the set of all nonnegative integer solutions $b = (b_1, b_2, ..., b_n)$ to the given equation described as follows. Given a partition of $n$, $a = (a_1, a_2, ..., a_k)$ for some $k \leq n$ such that $a_i \geq a_{i+1} > 0$ for all $i$, we obtain a nonnegative integer solution $b = (b_1, b_2, ..., b_n)$ in the following way. For each $j = 1, 2, ..., n$, we set $b_j$ to be equal to the number of times $j$ occurs in the partition $a$. Then clearly,

$$\sum_{j=1}^{n} jb_j = \sum_{i=0}^{k} a_i = n$$

whence $b$ is a solution. It is easily seen that the mapping $a \mapsto b$ is a bijection. □

### 3.1.1 Monomial Vectors

Lemma 3.1.1 motivates us to define a collection of vectors $I(\mu, r) \subset \mathbb{Z}_{\geq 0}^{r}$ associated to each positive power $\mu$ of a variable $y$ taking values in $\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ as follows. A vector $k = (k_0, k_1, ..., k_{r-1}) \in I(\mu, r)$ if on writing $y = y_0 + y_1 p + ... + y_{r-1}p^{r-1}$ the monomial $y_0^{k_0} y_1^{k_1} ... y_{r-1}^{k_{r-1}}$ occurs in the multinomial expansion of $(y_0 + y_1 p + ... + y_{r-1}p^{r-1})^{\mu} \pmod{p^r}$. The set $I(\mu, r)$ can be computed by using Lemma 3.1.1. And on $I(\mu, r)$, we define the map $d : I(\mu, r) \to \{0, 1, ..., r-1\}$ which sends $k = (k_0, k_1, ..., k_{r-1}) \mapsto \sum_{j=0}^{r-1} jk_j$ so that $d(k)$ gives the exponent of $p$ for which the monomial $y_0^{k_0} y_1^{k_1} ... y_{r-1}^{k_{r-1}}$ is the coefficient in the

multinomial expansion. For convenince, let us refer to any $k \in I(\mu, r)$ as a **monomial vector**.

In order to better understand the structure of $I(\mu, r)$, let us consider the following example. Let $\mu = 3, r = 4$ and $M$ be the $4 \times 7$ matrix,

$$\left[\begin{array}{c|c|cc|ccc} 3 & 2 & 2 & 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

so that the columns of $M$ are the elements in $I(3, 4)$. Notice that we divided the matrix into four blocks each corresponding to a $p$-power. That is, the monomial vectors belonging to the same block correspond to the monomials that occur as coefficients of the same $p$-power in the multinomial expansion assuming that none of the multinomial coefficients is divisible by $p$. The first block consists of a single column that corresponds to the monomial $y_0^3$. The second block consists of a single column that corresponds to the monomial $y_0^2 y_1$ that is obtained by applying the derivation in Lemma 3.1.1 to the columns in the first block. And similarly, the third block consists of the two columns that are *derived from* the columns in the previous (the second) block, and so on.

Hence, it makes sense to partition $I(\mu, r)$ as

$$I(\mu, r) = I_1(\mu, r) \amalg I_2(\mu, r) \amalg \ldots \amalg I_r(\mu, r) \tag{3.1.2}$$

where $I_1(\mu, r) = \{(\mu, 0, 0, ..., 0)\}$ and for each $i$ such that $2 \leq i \leq r$, $I_i(\mu, r)$ is the collection of vectors derived from $I_{i-1}(\mu, r)$ as per Lemma 3.1.1. Thus, in the (typical, worst) case when none of the multinomial coefficients are divisible by $p$, $I_j(\mu, r)$ consists of those monomials that are coefficients of $p^j$ occurring in the multinomial expansion. Then with the decomposition in equation 3.1.2, Lemma 3.1.3 implies the following proposition.

**Proposition 3.1.4.**
*Let $\mu$ be a positive integer. For any nonnegative integer $n$, let $P(n)$ denote the number of partitions of $n$. (Recall that $P(0) = 1$ by convention). Let $I(\mu, r)$ be decomposed as*

*in equation 3.1.2. Then we have the following.*

*(a) If $\mu \geq r-1$, then the cardinality of $I_r(\mu, r)$ is $P(r-1)$.*

*(b) For each $i$ such that $1 \leq i \leq r$, the cardinality of $I_i(\mu, r)$ is the cardinality of $I_i(\mu, i)$.*

*(c) If $\mu \geq r-1$, then the cardinality of $I(\mu, r)$ is $\sum_{j=0}^{r-1} P(j)$.*

*(d) If $\mu < r-1$, then the cardinality of $I_r(\mu, r)$ is strictly less than $P(r-1)$ and hence the cardinality of $I(\mu, r)$ is strictly less than $\sum_{j=0}^{r-1} P(j)$.*

*Proof.*

For part $(a)$, first assume $r > 1$ and recall that $I_r(\mu, r)$ is the collection of monomial vectors corrsponding to the monomials occurring as coefficients of $p^{r-1}$ in the expansion of $(y_0 + y_1 p + ... + y_{r-1}p^{r-1})^\mu$. Observe that when $\mu \geq r-1$, the monomials vectors in $I_r(\mu, r)$ can be obtained by successively applying the derivation in Lemma 3.1.1 to $I_i(\mu, r)$ for $i = 1, 2, ..., r-1$, and these corresponds to *all* the monomials obtained from $y_0^\mu$ through differentiation using the *usual Leibniz rule* since the least possible exponent of $y_0$ (obtained by applying the derivation in Lemma 3.1.1 $(r-1)$ times) is $\mu-(r-1)$ which is nonnegative. In this case, the cardinality of $I_r(\mu, r)$ is precisely the number of ways of choosing a collection of elements (with repetitions) from the set $\{y_0, y_1 p, ..., y_{r-1}p^{r-1}\}$ such that the power of $p$ of the product of the chosen elements is exactly $p^{r-1}$ and this is same as the number of nonnegative integer solutions to the equation

$$\sum_{j=1}^{n} j b_j = r-1 \tag{3.1.3}$$

where $b_j$ refers to the number of repetitions of the term $y_j p^j$ that occurs in the product (of the chosen elements). By Lemma 3.1.3, this number is $P(r-1)$. In other words, if $S$ is the set of all nonnegative solutions to equation 3.1.3, then the map $h : I_r(\mu, r) \to S$ defined by $h(k) = (k_1, k_2, ..., k_{r-1})$ is a bijection. (For the case when $r = 1$ it is trivial to check that $I_r(\mu, r)$ has cardinality $P(0) = 1$).

Part $(b)$ trivially follows from the definitions of $I_i(\mu, r)$ and $I_i(\mu, i)$ along with Lemma 3.1.1. Part $(a)$ along with part $(b)$ and equation 3.1.2 implies part $(c)$. Finally, when

$\mu < r-1$, then on one hand, every monomial vector in $I_r(\mu, r)$ corresponds to a unique nonnegative soluton of equation 3.1.3. In other words, if $S$ is the set of all nonnegative solutions to equation 3.1.3, then the map $h : I_r(\mu, r) \to S$ defined by $h(k) = (k_1, k_2, ..., k_{r-1})$ is injective. However the map is not surjective since *not all* nonnegative solutions to equation 3.1.3 give rise to monomial vectors, for example, the vector $(\mu-(r-1), r-1, 0, 0, ..., 0)$ is not in $I(\mu, r)$ since the first coordinate is negative. Hence we have part $(d)$. □

For each $\mu \in \{1, 2, ..., m\}$, it is often convenient to represent $I(\mu, r)$ as a matrix $M(\mu, r)$ whose columns are the elements of $I(\mu, r)$, arranged in a lexicographic order starting from $I_1(\mu, r)$ to $I_r(\mu, r)$ where the columns corresponding to each of the $I_i(\mu, r)$ are again arranged in a lexicographic order determined be the corresponding partitions of $(i-1)$.

For example, for $\mu = 5$ and $r = 4$, we have

$$M(5,4) = \left[\begin{array}{c|c|ccc|ccc} 5 & 4 & 4 & 4 & 4 & 3 & 3 \\ 0 & 1 & 0 & 2 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

and for $\mu = 1$ and $r = 4$, we have

$$M(1,4) = \left[\begin{array}{c|c|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

and in general, we have for sufficiently large $\mu$,

$$M(\mu, 1) = \left[\mu\right],$$

$$M(\mu,2)=\left[\begin{array}{c|c}\mu & \mu-1\\ 0 & 1\end{array}\right],$$

$$M(\mu,3)=\left[\begin{array}{c|c|cc}\mu & \mu-1 & \mu-1 & \mu-2\\ 0 & 1 & 0 & 2\\ 0 & 0 & 1 & 0\end{array}\right],$$

$$M(\mu,4)=\left[\begin{array}{c|c|cc|ccc}\mu & \mu-1 & \mu-1 & \mu-1 & \mu-1 & \mu-2 & \mu-2\\ 0 & 1 & 0 & 2 & 0 & 1 & 3\\ 0 & 0 & 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0\end{array}\right],$$

and so on. It is easy to see from 3.1.2 and by the definition of $M(\mu,r)$ that the following lemma holds.

**Lemma 3.1.5.**

*Given $\mu \in \{1,2,...,m\}$, for each $r \geq 2$, the matrix $M(\mu,r)$ is obtained from the matrix $M(\mu,r-1)$ by first appending an all-zero row and then appending new columns obtained by applying Lemma 3.1.1 to the monomials corresponding to the columns in $M(\mu,r-1)$ and then arranging these columns in the lexicographic order determined by the corresponding partitions or $(r-1)$. That is,*

$$M(\mu,r)=\begin{bmatrix}M(\mu,r-1) & \textit{Lemma 3.1.1} \circ M(\mu,r-1)\\ \mathbf{0} & \textit{Lemma 3.1.1} \circ M(\mu,r-1)\end{bmatrix}.$$

### 3.1.2 Growth of Coefficients of the Power Series associated to $\bar{f}$

With the above definition of monomial vectors, we may rewrite the polynomial $\bar{f}(\bar{x})$ in terms of *Teichmüller variables* $(x_j)_{0\leq j\leq r-1}$ whenever $\bar{x}$ is a variable taking values in $(\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l})$ as follows:

$$\begin{aligned}
\bar{f}(\bar{x}) &= \sum_{\mu=1}^{m} \bar{a}_\mu \bar{x}^\mu \\
&= \sum_{\mu=1}^{m} \sum_{s=0}^{r-1} a_{\mu,s} p^s \left( \sum_{j=0}^{r-1} x_j p^j \right)^\mu \\
&= \sum_{\mu=1}^{m} \sum_{s=0}^{r-1} a_{\mu,s} p^s \sum_{k \in I(\mu,r)} c_{\mu,k} \left( \prod_{j=0}^{r-1} x_j^{k_j} \right) p^{d(k)} \\
&= \sum_{\mu=1}^{m} \sum_{k \in I(\mu,r)} \sum_{s=0}^{r-1} a_{\mu,s} c_{\mu,k} x^k p^{d(k)+s} \qquad (3.1.4)
\end{aligned}$$

for some integer coefficients $c_{\mu,k}$, where the variable $\bar{x}$ has its $p$-adic expansion in terms of Teichmüller variables $x_0, x_1, ..., x_{r-1}$ given by $\bar{x} = \sum_{j=0}^{r-1} x_j p^j$, and $\sum_{s=0}^{r-1} a_{\mu,s} p^s$ is the $p$-adic representation of the $\bar{a}_\mu$ in terms of Teichmüller digits, $a_{\mu,s}$.

Now, if $\bar{x} \in (\mathbb{Z}_{q^l}/p^r \mathbb{Z}_{q^l})$ and if we denote the vector of Teichmüller variables $(x_0, x_1, ..., x_{r-1})$ by $x$, then applying the character $\Theta_r \circ \tau(q,l,r)$ to $\bar{f}(\bar{x})$ we get

$$\begin{aligned}
\Theta^{(r)} \circ \tau(q,l,r) \left( \bar{f}(\bar{x}) \right) &= \prod_{\mu=1}^{m} \prod_{k \in I(\mu,r)} \prod_{s=0}^{r-1} \left[ \Theta^{(r)} \circ \tau(q,l,r) \left( a_{\mu,s} x^k p^{d(k)+s} \right) \right]^{c_{\mu,k}} \\
&= \prod_{\mu=1}^{m} \prod_{u=0}^{r-1} \prod_{\substack{k \in I(\mu,r) \\ 0 \le s \le r-1 \\ d(k)+s=u}} \left[ \Theta^{(r)} \circ \tau(q,l,r) \left( a_{\mu,s} x^k p^u \right) \right]^{c_{\mu,k}} \\
&= \prod_{\mu=1}^{m} \prod_{u=0}^{r-1} \prod_{\substack{k \in I(\mu,r) \\ 0 \le s \le r-1 \\ d(k)+s=u}} \left[ \prod_{j=0}^{al-1} \theta_{r-u}(a_{\mu,s}^{p^j} x^{kp^j}) \right]^{c_{\mu,k}} \\
&= \prod_{\mu=1}^{m} \prod_{u=0}^{r-1} \prod_{\substack{k \in I(\mu,r) \\ 0 \le s \le r-1 \\ d(k)+s=u}} \left[ \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} \theta_{r-u}(a_{\mu,s}^{p^j} x^{kp^{ia+j}}) \right]^{c_{\mu,k}} \\
&= \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} \prod_{\mu=1}^{m} \prod_{u=0}^{r-1} \prod_{\substack{k \in I(\mu,r) \\ 0 \le s \le r-1 \\ d(k)+s=u}} \left[ \theta_{r-u}(a_{\mu,s}^{p^j} x^{kp^{ia+j}}) \right]^{c_{\mu,k}} \qquad (*)
\end{aligned}$$

where the third equality follows from Theorem 2.1.18 and the fourth equality follows from the fact that $a_{\mu,s}^{q} = a_{\mu,s}$, and hence we have obtained an analogue of Proposition 2.1.21 in the previous chapter.

**Definition 3.1.6.** For each $i \in \{0, 1, ..., l-1\}$ and for each $j \in \{0, 1, ..., a-1\}$, we define

$$\boxed{F_{i,j}(x) := \prod_{\mu=1}^{m} \prod_{u=0}^{r-1} \prod_{\substack{k \in I(\mu,r) \\ 0 \leq s \leq r-1 \\ d(k)+s=u}} \left[\theta_{r-u}(a_{\mu,s}^{p^j} x^{kp^{ia+j}})\right]^{c_{\mu,k}}} \tag{3.1.5}$$

where $x = (x_0, x_1, ..., x_{r-1})$, the $a_{\mu,s}$ are the Teichmüller digits of the coefficients $\bar{a}_\mu$ as defined before and the $c_{\mu,k}$ are the integer coefficients obtained from the multinomial expansions as discussed before.

With the above definition we have

$$\Theta^{(r)} \circ \tau(q, l, r)\left(\bar{f}(\bar{x})\right) = \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} F_{i,j}(x) \tag{3.1.6}$$

Let us now analyze the growth of the coefficients of the basic series $F_{0,0}(x)$. In order to emphasize the degree, $m$ of the polynomial, $\bar{f}$ (which is useful in determining the weight functions) it is sometimes useful to incorporate that into the notation. Consider

$$\boxed{F_{0,0}^{(m)}(x) := F_{0,0}(x) = \prod_{\mu=1}^{m} \prod_{u=0}^{r-1} \prod_{\substack{k \in I(\mu,r) \\ 0 \leq s \leq r-1 \\ d(k)+s=u}} \left[\theta_{r-u}(a_{\mu,s} x^k)\right]^{c_{\mu,k}}}.$$

It is useful to rewrite the product as follows.

$$F_{0,0}^{(m)}(x) = \prod_{\mu=1}^{m} \prod_{s=0}^{r-1} \prod_{k \in I(\mu,r,s)} \left[\theta_{r-d(k)-s}(a_{\mu,s} x^k)\right]^{c_{\mu,k}}.$$

where $I(\mu, r, s)$ is the subset of $I(\mu, r)$ consisting of those monomial vectors $k$ for which $d(k) < r - s$. Now for fixed $(\mu, s)$ let

$$F_{0,0}^{(\mu,r,s)}(x) := \prod_{k \in I(\mu,r,s)} \left[\theta_{r-d(k)-s}(a_{\mu,s} x^k)\right]^{c_{\mu,k}} \tag{3.1.7}$$

Then we have the following proposition.

**Proposition 3.1.7.**

$$F_{0,0}^{(\mu,r,s)}(x) = \prod_{k\in I(\mu,r,s)} \sum_{h^{(k)}=0}^{\infty} B_{(\mu,r,s)}(k,h^{(k)}) x^{kh^{(k)}}$$

*where the coefficients* $B_{(\mu,r,s)}(k,h^{(k)})$ *satisfy*

$$\operatorname{ord}_p B_{(\mu,r,s)}(k,h^{(k)}) \geq \frac{h^{(k)}}{p^{r-d(k)-s-1}(p-1)} \geq \frac{h^{(k)}}{p^{r-d(k)-1}(p-1)}.$$

*Proof.* We recall that the integer $c_{\mu,k}$ is simply the multinomial coefficient, $\binom{\mu}{k_0,k_1,\ldots,k_{r-1}}$. Then for some coefficients $b_h^{(r-d(k)-s)}$,

$$\begin{aligned} F_{0,0}^{(\mu,r,s)}(x) &= \prod_{k\in I(\mu,r,s)} \left( \sum_{h=0}^{\infty} b_h^{(r-d(k)-s)} x^{kh} \right)^{c_{\mu,k}} \\ &= \prod_{k\in I(\mu,r,s)} \prod_{j=1}^{c_{\mu,k}} \sum_{h_j=0}^{\infty} b_{h_j}^{(r-d(k)-s)} x^{kh_j} \\ &= \prod_{k\in I(\mu,r,s)} \sum_{h^{(k)}=0}^{\infty} B_{(\mu,r,s)}(k,h^{(k)}) x^{kh^{(k)}} \end{aligned}$$

where

$$B_{(\mu,r,s)}(k,h^{(k)}) = \sum \prod_{j=1}^{c_{\mu,k}} b_{h_j}^{(r-d(k)-s)}$$

where the sum runs over $\mathbf{h} = (h_1, h_2, ..., h_{c_{\mu,k}}) \in \mathbb{Z}_{\geq 0}^{c_{\mu,k}}$ such that $\sum_{j=1}^{c_{\mu,k}} h_j = h^{(k)}$. And we have

$$\begin{aligned} \operatorname{ord}_p B_{(\mu,r,s)}(k,h^{(k)}) &\geq \inf \left\{ \sum_{j=1}^{c_{\mu,k}} \operatorname{ord}_p b_{h_j} : \sum_{j=1}^{c_{\mu,k}} h_j = h^{(k)} \right\} \\ &\geq \sum_{j=1}^{c_{\mu,k}} \frac{h_j}{p^{r-d(k)-s-1}(p-1)} \\ &= \frac{h^{(k)}}{p^{r-d(k)-s-1}(p-1)} \end{aligned}$$

by the $p$-adic analytic properties of the function $\theta_{r-d(k)-s}(t)$ established earlier. □

Following the description above, we have

$$F_{0,0}^{(m)}(x) = \prod_{\mu=1}^{m}\prod_{s=0}^{r-1}\prod_{k\in I(\mu,r,s)}\left[\theta_{r-d(k)-s}(a_{\mu,s}x^k)\right]^{c_{\mu,k}}$$
$$= \prod_{\mu=1}^{m}\prod_{s=0}^{r-1}\prod_{k\in I(\mu,r,s)}\sum_{h^{(k)}=0}^{\infty} B_{(\mu,r,s)}(k,h^{(k)})x^{kh^{(k)}}$$

for some coefficients $B_{(\mu,r,s)}(k,h^{(k)})$ satisfying $\operatorname{ord}_p B_{(\mu,r,s)}(k,h^{(k)}) \geq \dfrac{h^{(k)}}{p^{r-d(k)-s-1}(p-1)}$ by Proposition 3.1.7. Rewriting $F_{0,0}^{(m)}(x)$ as a series,

$$\boxed{F_{0,0}^{(m)}(x) = \sum_{\kappa\in\mathbb{Z}_{\geq 0}^{r}} A(\kappa)x^{\kappa}}$$

we see that the coefficients $A(\kappa)$ are given as follows.

**Definition 3.1.8.** We say that the polynomial $f(x) \in \mathbb{Q}_q[x_0, x_1, ..., x_{r-1}]$ is the **$r$-expansion** of $\bar{f}(\bar{x})$ if $f(x)$ is the last expression in Equation 3.1.4 with the coefficients $c_{\mu,k}$ being the multinomial coefficients $\binom{\mu}{k_0,k_1,\ldots,k_{r-1}}$.

**Definition 3.1.9.** Let $J(\bar{f}, r, \kappa)$ be the set of all solutions in $\mathbb{Z}_{\geq 0}^{r}$ to the system of equations

$$K(\bar{f}, r)\cdot h = \kappa \tag{3.1.8}$$

where $K(\bar{f}, r)$ is a matrix with $r$ rows and whose columns are all the possible monomial vectors occurring in the $r$-expansion of $\bar{f}(\bar{x})$. It is convenient to index the columns as $k^{(s,\mu,i_{(s,\mu)})}$ where $s$ runs from 0 through $r-1$, $\mu$ runs from 1 through $m$, and for each fixed pair $(s,\mu)$, $i_{(s,\mu)}$ runs from 1 through the cardinality of $I(\mu,r,s)$ which we denote by $\bar{\rho}(\mu,r,s)$. In this way, it is useful to think of the matrix $K(\bar{f}, r)$ as consisting of $r$ blocks, one each for $s = 0, 1, 2, ..., r-1$; arranged from left to right.

The following lemma is useful in computing $K(\bar{f}, r)$ recursively.

**Lemma 3.1.10.**

*For each $r \geq 2$, the matrix $K(\bar{f}, r)$ is obtained from the matrix $K(\bar{f}, r-1)$ by first append-*

*ing an all-zero row and then appending new columns obtained by applying Lemma 3.1.1 to the monomials corresponding to the columns in* $K(\bar{f}, r-1)$ *for each* $\mu \in \{1, 2, ..., m\}$ *and then finally repeating all the columns of* $K(\bar{f}, r-1)$, $K(\bar{f}, r-2)$ *and so on until* $K(\bar{f}, 1)$ *with an all-zero row appended. That is,*

$$K(\bar{f}, r) = \left[\begin{array}{c|c|c|c|c|c} K(\bar{f}, r-1) & \textit{Lemma 3.1.1} \circ K(\bar{f}, r-1) & K(\bar{f}, r-1) & K(\bar{f}, r-2) & \dots & K(\bar{f}, 1) \\ \mathbf{0} & \textit{Lemma 3.1.1} \circ K(\bar{f}, r-1) & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array}\right]$$

Before we state the proof of this lemma, here is an example to see how this lemma works. Let $m = 4$. Then we have:

$$K(\bar{f}, 1) = \begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix},$$

$$K(\bar{f}, 2) = \left[\begin{array}{cc|cc|cc|cc||cccc} 1 & 0 & 2 & 1 & 3 & 2 & 4 & 3 & 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right],$$

$$K(\bar{f}, 3) = \left[\begin{array}{ccc|ccc|ccc|ccc||cc|cc|cc|cc||cccc} 1 & 0 & 0 & 2 & 1 & 1 & 0 & 3 & 2 & 2 & 1 & 4 & 3 & 3 & 2 & 1 & 0 & 2 & 1 & 3 & 2 & 4 & 3 & 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right],$$

and so on. $K(\bar{f}, 1)$ has just one "big block", corresponding to $s = 0$. $K(\bar{f}, 2)$ has two "big blocks" (demarcated by $||$), the leftmost corresponding to $s = 0$ and the rightmost corresponding to $s = 1$. In other words, $K(\bar{f}, 3)$ can be broken as

$$K(\bar{f}, 2) = \left[K_0(\bar{f}, 2) \;\middle\|\; K_1(\bar{f}, 2)\right]$$

where

$$K_0(\bar{f}, 2) = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 2 & 1 & 3 & 2 & 4 & 3 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right], \text{ and}$$

$$K_1(\bar{f},2) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Likewise, $K(\bar{f},3)$ has three "big blocks" (demarcated by ||), the leftmost corresponding to $s=0$, the middle one corresponding to $s=1$, and the rightmost corresponding to $s=2$. In other words, $K(\bar{f},3)$ can be broken as

$$K(\bar{f},3) = \Big[ K_0(\bar{f},3) \,\Big\|\, K_1(\bar{f},3) \,\Big\|\, K_2(\bar{f},3) \Big]$$

where

$$K_0(\bar{f},3) = \left[\begin{array}{ccc|cccc|cccc|cccc} 1 & 0 & 0 & 2 & 1 & 1 & 0 & 3 & 2 & 2 & 1 & 4 & 3 & 3 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}\right],$$

$$K_1(\bar{f},3) = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 2 & 1 & 3 & 2 & 4 & 3 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right], \text{ and}$$

$$K_2(\bar{f},3) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

We thus observe that $K(\bar{f},2)$ is obtained as follows. $K_0(\bar{f},2)$ is just all the monomial vectors in $K(\bar{f},1)$ appended with 0 (for the new Teichmüller variable, $x_1$) along with the new monomials derived from these using Lemma 3.1.5. And $K_1(\bar{f},2)$ is just all the monomial vectors in $K(\bar{f},1)$ appended with 0 and nothing more, for there is already a $p$-power due to $s=1$, and we can afford no more $p$ powers when $r=2$.

Similarly, $K(\bar{f},3)$ is obtained as follows. $K_0(\bar{f},3)$ is just all the monomial vectors in $K(\bar{f},2)$ appended with 0 (for the new Teichmüller variable, $x_2$) along with the new monomials derived from these using Lemma 3.1.5. And $K_1(\bar{f},3)$ is just all the monomial vectors in $K(\bar{f},2)$ appended with 0 and nothing more due to $s=1$, and any additional monomials will have a higher $p$-power. Finally, $K_2(\bar{f},3)$ is just all the monomial vectors in $K(\bar{f},1)$ appended with 0 and nothing more due to $s=2$, again since any additional

monomials will have a higher $p$-power.

We are now ready to understand the proof of Lemma 3.1.10 better.

*Proof of the lemma.* That the first block in the matrix $K(\bar{f}, r)$ corresponding to $s = 0$ is obtained in the way described follows from Lemma 3.1.5. Then the block corresponding to each $s > 1$ (having an intrinsic $p$-power, namely, $p^s$ associated to it) is precisely given by the block

$$\begin{bmatrix} K(\bar{f}, r-s) \\ \mathbf{0} \end{bmatrix}$$

for the monomials corresponding to those columns are the only ones for which the corresponding $p$-power is less than or equal to $r - s - 1$ and $p^{r-s-1}p^s = p^{r-1}$, the maximum affordable $p$-power. □

Then we have

$$\begin{aligned} A(\kappa) &= \sum_{h \in J(\bar{f},r,\kappa)} \prod_{\mu=1}^{m} \prod_{s=0}^{r-1} \prod_{k \in I(\mu,r,s)} B_{(\mu,r,s)}(k, h^{(k)}) \\ &= \sum_{h \in J(\bar{f},r,\kappa)} \prod_{s=0}^{r-1} \prod_{\mu=1}^{m} \prod_{k \in I(\mu,r,s)} B_{(\mu,r,s)}(k, h^{(k)}) \\ &= \sum_{h \in J(\bar{f},r,\kappa)} \prod_{s=0}^{r-1} \prod_{\mu=1}^{m} \prod_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} B_{(\mu,r,s)}(k^{(s,\mu,i_{(s,\mu)})}, h^{(s,\mu,i_{(s,\mu)})}) \\ &= \sum_{h \in J(\bar{f},r,\kappa)} \prod_{s=0}^{r-1} \prod_{\mu=1}^{m} \prod_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} B_{(\mu,r,s)}(k^{(s,\mu,i_{(s,\mu)})}, h_{s,\mu,i_{(s,\mu)}}) \end{aligned} \tag{3.1.9}$$

where the last equation is for notational convenience (let us write $h_{s,\mu,i_{(s,\mu)}}$ for $h^{(s,\mu,i_{(s,\mu)})}$ both denoting the $(s, \mu, i_{(s,\mu)})$-th component of the vector $h$). Using Proposition 3.1.7 we obtain the following estimate (Proposition 3.1.12) on the $p$-adic size of the coefficients $A(\kappa)$. Before we state the proposition let us first define $J_{\mathbb{Q}}(\bar{f}, r, \kappa)$ to be the set of all solutions in $\mathbb{Q}^c_{\geq 0}$, where $c = \sum_{\mu=1}^{m} \sum_{s=0}^{r-1} \bar{\rho}(\mu, r, s)$ is the number of columns of the matrix $K(\bar{f}, r)$, to the system of equations 3.1.8. Let us also define a weight functiton as follows.

**Definition 3.1.11.** For each $\kappa \in \mathbb{Z}^r_{\geq 0}$, define $w(\kappa)$ to be

$$w(\kappa) = \inf_{h \in J_{\mathbb{Q}}(\bar{f},r,\kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \left( \frac{1}{p^{r-1}} \right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\}.$$

We say that $w(\kappa)$ is the *weight* of $\kappa$.

**Proposition 3.1.12.** *With the above definitions, we have*

$$\operatorname{ord}_p A(\kappa) \geq \frac{w(\kappa)}{p-1}.$$

*Proof.* From Equation 3.1.9, on using Proposition 3.1.7, we have

$$\begin{aligned}
\operatorname{ord}_p A(\kappa) &\geq \inf_{h \in J(\bar{f},r,\kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \operatorname{ord}_p B_{(\mu,r,s)}(k^{(s,\mu,i_{(s,\mu)})}, h_{(s,\mu,i_{(s,\mu)})}) \right\} \\
&\geq \inf_{h \in J(\bar{f},r,\kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \frac{h_{(s,\mu,i_{(s,\mu)})}}{p^{r-d(k^{(s,\mu,i_{(s,\mu)})})-s-1}(p-1)} \right\} \\
&= \inf_{h \in J(\bar{f},r,\kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \frac{p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})}}{p^{r-1}(p-1)} \right\} \\
&= \left( \frac{1}{p-1} \right) \cdot \inf_{h \in J(\bar{f},r,\kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \left( \frac{1}{p^{r-1}} \right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\} \\
&\geq \left( \frac{1}{p-1} \right) \cdot \inf_{h \in J_{\mathbb{Q}}(\bar{f},r,\kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \left( \frac{1}{p^{r-1}} \right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\} \\
&= \frac{w(\kappa)}{p-1}.
\end{aligned}$$

□

We make the observation that the weight function $w : \mathbb{Z}^r_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined above (Definition 3.1.11) is an "intuitive" weight function that satisfies the following properties for $\kappa, \kappa_1, \kappa_2 \in \mathbb{Z}^r_{\geq 0}$ and for $c \geq 0$:

(i) $w(\kappa) = 0 \iff \kappa = 0$

(ii) $w(c\kappa) = cw(\kappa)$

(iii) $w(\kappa_1 + \kappa_2) \leq w(\kappa_1) + w(\kappa_2)$

The third property is not as easily seen as the other two. The following lemma helps.

**Lemma 3.1.13.** *Let $K$ be an $r \times c$ matrix with $c \geq 1$ and with entries in $\mathbb{Q}_{\geq 0}$. For each $\kappa \in \mathbb{Z}^r_{\geq 0}$, let $J(\kappa)$ be the set of all solutions in $\mathbb{Q}^c_{\geq 0}$ of the matrix equation $Kh = \kappa$, and let $v : \mathbb{Z}^r_{\geq 0} \to \mathbb{R}_{\geq 0}$ be a function defined by*

$$v(\kappa) := \inf\{\ell(h) : h \in J(\kappa)\}$$

*where $\ell(h)$ is a linear form in $h$ with coefficients in $\mathbb{Q}_{\geq 0}$. Then for $\kappa_1, \kappa_2 \in \mathbb{Z}^r_{\geq 0}$, we have*

$$v(\kappa_1 + \kappa_2) \leq v(\kappa_1) + v(\kappa_2).$$

*Proof.* If $h_1 \in J(\kappa_1)$ and $h_2 \in J(\kappa_2)$, then clearly $h_1 + h_2 \in J(\kappa_1 + \kappa_2)$. Thus, if $J(\kappa_1)$ and $J(\kappa_2)$ are both nonempty, $J(\kappa_1 + \kappa_2)$ is nonempty and

$$v(\kappa_1 + \kappa_2) \leq \ell(h_1 + h_2) = \ell(h_1) + \ell(h_2).$$

The above inequality is true for *all* $h_1 \in J(\kappa_1)$ and for *all* $h_2 \in J(\kappa_2)$. It follows that

$$v(\kappa_1 + \kappa_2) \leq v(\kappa_1) + v(\kappa_2).$$

The inequality holds trivially when either of $J(\kappa_1)$ and $J(\kappa_2)$ is empty, then the above inequality holds trivially. □

We now define a *diagrammatic* weight function which we later show is a good estimate for the weight function defined above. For the case when $r = 1$, the *Newton polyhedral* (diagram) weight function [AS87a] that we defined in Chapter 2 coincides with an "intuitive" analytical weight function as we saw in Corollary 2.2.4. However, for $r > 1$, we will see that the following *diagram* weight function does not coincide with the "intuitive" analytical weight function (Definition 3.1.11), but merely approximates it.

**Definition 3.1.14.** For $y = (y_0, y_1, ..., y_{r-1}) \in \mathbb{Z}^r_{\geq 0}$, define the following:

- $w_1(y) := py_1 + p^2y_2 + ... + p^{r-1}y_{r-1} = \sum_{j=1}^{r-1} p^j y_j$.
- $w_2(y) := \left(\frac{1}{m}\right) y_0 + \left(p - \frac{m-1}{m}\right) y_1 + ... + \left(p^{r-1} - \frac{m-1}{m}\right) y_{r-1} = \sum_{j=0}^{r-1} \left(p^j - \frac{m-1}{m}\right) y_j$.
- $w_\Delta(y) := \max\{w_1(y), w_2(y)\}$.

We say that $w_\Delta(y)$ is the **level-$r$ $\Delta$-diagram weight** of $y$. The reasons for this nomenclature will soon become clear as soon as we see the special cases when $r = 2$ and $r = 3$.

At this point, let us consider the special cases when $r = 2$ and $r = 3$ and eventually observe the general pattern in order to define a good diagram weight function that helps us build $p$-adic Banach spaces leading to a trace formula.

### 3.1.3 The case when $r = 2$

In this case, we have that $s$ runs from 0 through 1 and for each $\mu = 1, 2, ..., m$, we have $I(\mu, 2, 0) = \{(\mu, 0), (\mu-1, 1)\}$ and $I(\mu, 2, 1) = \{(\mu, 0)\}$. Thus the matrix $K(\bar{f}, 2)$ consists of (a maximum of) $2m + m = 3m$ columns. Let us write out the matrix as

$$\left[\begin{array}{cc|cc|c|cc||cccc} 1 & 0 & 2 & 1 & \dots & m & m-1 & 1 & 2 & \dots & m \\ 0 & 1 & 0 & 1 & \dots & 0 & 1 & 0 & 0 & \dots & 0 \end{array}\right]$$

where the first big block (demarcated by $||$) corresponds to $s = 0$ and the next big block corresponds to $s = 1$. Then the system of equations

$$K(\bar{f}, r) \cdot h = \kappa$$

read as follows.

$$\begin{aligned} &[h_{(0,1,1)} + 2h_{(0,2,1)} + 3h_{(0,3,1)} + \dots + mh_{(0,m,1)}] \\ +&[0 + h_{(0,2,2)} + 2h_{(0,3,2)} + \dots + (m-1)h_{(0,m,2)}] \\ +&[h_{(1,1,1)} + 2h_{(1,2,1)} + 3h_{(1,3,1)} + \dots + mh_{(1,m,1)}] = \kappa_0 \end{aligned} \tag{3.1.10}$$

$$h_{(0,1,2)} + h_{(0,2,2)} + \ldots + h_{(0,m,2)} = \kappa_1 \tag{3.1.11}$$

Let us now obtain a bound for $w(\kappa)$ and hence for $\operatorname{ord}_p A(\kappa)$ in terms of the diagram weight $w_\Delta(\kappa)$ for the case when $r = 2$.

At this moment we present a geometric interpretation of the diagram weight hence justifying the name.

**Definition 3.1.15.** For each column, $k$ of the matrix $K(\bar{f}, r)$, (see Definition 3.1.9), divide its components by $p^{d(k)+s}$ where we recall that $d(k) = \sum_{j=1}^{r-1} jk_j$ is the exponent of $p$ corresponding to the monomial vector $k$, and $s$ is the *block* in which $k$ is in. Let $K_\Delta(\bar{f}, r)$ be the new matrix obtained after this division.

Then, for $r = 2$, we have

$$K_\Delta(\bar{f}, 2) = \left[\begin{array}{cc|cc|c|cc||cccc} 1 & 0 & 2 & \binom{1}{p} & \ldots & m & \binom{m-1}{p} & \binom{1}{p} & \binom{2}{p} & \ldots & \binom{m}{p} \\ 0 & \binom{1}{p} & 0 & \binom{1}{p} & \ldots & 0 & \binom{1}{p} & 0 & 0 & \ldots & 0 \end{array}\right]$$

We similarly obtain the matrix $K_\Delta(\bar{f}, r)$ for all $r \geq 2$. For our example, when $m = 4$, we have

$$K_\Delta(\bar{f}, 1) = \begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix},$$

$$K_\Delta(\bar{f}, 2) = \left[\begin{array}{cc|cc|cc|cc||cccc} 1 & 0 & 2 & \frac{1}{p} & 3 & \frac{2}{p} & 4 & \frac{3}{p} & \frac{1}{p} & \frac{2}{p} & \frac{3}{p} & \frac{4}{p} \\ 0 & \frac{1}{p} & 0 & \frac{1}{p} & 0 & \frac{1}{p} & 0 & \frac{1}{p} & 0 & 0 & 0 & 0 \end{array}\right], \text{ and}$$

$$K_\Delta(\bar{f}, 3) = \begin{bmatrix} K_{\Delta,0}(\bar{f}, 3) \,\|\, K_{\Delta,0}(\bar{f}, 3) \,\|\, K_{\Delta,0}(\bar{f}, 3) \end{bmatrix}$$

where

$$K_{\Delta,0}(\bar{f},3) = \left[\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 2 & \frac{1}{p} & \frac{1}{p^2} & 0 & 3 & \frac{2}{p} & \frac{2}{p^2} & \frac{1}{p^2} & 4 & \frac{3}{p} & \frac{3}{p^2} & \frac{2}{p^2} \\ 0 & \frac{1}{p} & 0 & 0 & \frac{1}{p} & 0 & \frac{2}{p^2} & 0 & \frac{1}{p} & 0 & \frac{2}{p^2} & 0 & \frac{1}{p} & 0 & \frac{2}{p^2} \\ 0 & 0 & \frac{1}{p^2} & 0 & 0 & \frac{1}{p^2} & 0 & 0 & 0 & \frac{1}{p^2} & 0 & 0 & 0 & \frac{1}{p^2} & 0 \end{array}\right],$$

$$K_{\Delta,1}(\bar{f},3) = \left[\begin{array}{cc|cc|cc|cc} \frac{1}{p} & 0 & \frac{2}{p} & \frac{1}{p^2} & \frac{3}{p} & \frac{2}{p^2} & \frac{4}{p} & \frac{3}{p^2} \\ 0 & \frac{1}{p^2} & 0 & \frac{1}{p^2} & 0 & \frac{1}{p^2} & 0 & \frac{1}{p^2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right], \text{ and}$$

$$K_{\Delta,2}(\bar{f},3) = \begin{bmatrix} \frac{1}{p^2} & \frac{2}{p^2} & \frac{3}{p^2} & \frac{4}{p^2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

We have the following proposition.

**Proposition 3.1.16.** *Let $m$ be a positive integer with $m > 1$. Let $S$ be the set of all columns of the matrix $K_\Delta(\bar{f},2)$ along with the zero vector. Then the convex hull of $S$ in $\mathbb{R}^2$ viewed as the $x_0x_1$-plane is simply the region bounded by the polygon with vertices $(0,\frac{1}{p}), (\frac{m-1}{p},\frac{1}{p}), (m,0)$ and $(0,0)$. And the faces of the polygon lie in the hyperplanes $x_0 = 0$, $x_1 = 0$, $w_1(x_0,x_1) = 1$ and $w_2(x_0,x_1) = 1$.*

**Remark 3.1.17.** Note that the convex hull of $S$ is the same as the convex hull of the set of all columns of $K_\Delta(\bar{f},2)$ that lie in the first ($s = 0$) block, along with the zero vector.

*Proof of Proposition 3.1.16.* The proof is trivial. (Observe that the hyperplane $w_1(x_0,x_1) = 1$ is precisely the straight line joining the points $(0,\frac{1}{p})$ and $(\frac{m-1}{p},\frac{1}{p})$ and the hyperplane $w_2(x_0,x_1) = 1$ is precisely the straight line joining the points $(\frac{m-1}{p},\frac{1}{p})$ and $(m,0)$.) $\square$

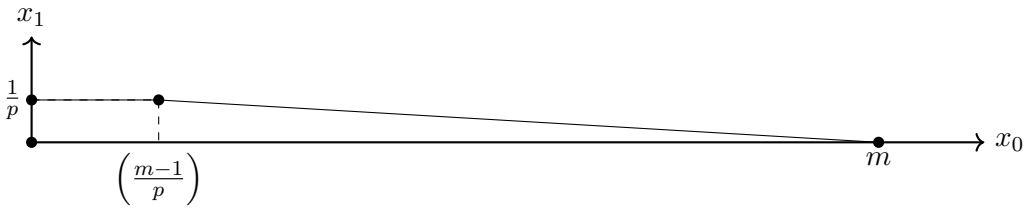



Figure 3.1: The level-2 $\Delta$-diagram corresponding to $\bar{f}$ with $m = 4$ and $p = 5$

Let us call the polygon in the previous proposition **the level-2 $\Delta$-diagram** of $\bar{f}$, and denote it by $\Delta(\bar{f}, 2)$. Please see the figure above for an example.

By the arguments similar to those in Proposition 2.2.2, one can show the following result.

**Proposition 3.1.18.** *For $y = (y_0, y_1) \in \mathbb{Z}^2_{\geq 0}$, $w_\Delta(y)$ is the smallest nonnegative rational number, $b$ such that the convex set $b\Delta(\bar{f}, 2) := \{b\alpha : \alpha \in \Delta(\bar{f}, 2)\}$ includes $y$.*

We now claim that the following is true.

**Proposition 3.1.19.** *For $\kappa = (\kappa_0, \kappa_1) \in \mathbb{Z}^2_{\geq 0}$, one has*

$$pw(\kappa) \geq w_\Delta(\kappa)$$

*Proof.* We have

$$\begin{aligned}
w(\kappa) &= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, r, \kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \left(\frac{1}{p^{r-1}}\right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\} \\
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, 2, \kappa)} \left\{ \sum_{s=0}^{1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,2)} \left(\frac{1}{p}\right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\} \\
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, 2, \kappa)} \left\{ \left(\frac{1}{p}\right) \sum_{\mu=1}^{m} h_{(0,\mu,1)} + \left[ \sum_{\mu=1}^{m} h_{(0,\mu,2)} + \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right] \right\} \\
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, 2, \kappa)} \left\{ \left(\frac{1}{p}\right) \sum_{\mu=1}^{m} h_{(0,\mu,1)} + \left[ \kappa_1 + \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right] \right\} \qquad (3.1.12)
\end{aligned}$$

where the last equality follows from Equation 3.1.11.

Now if $h \in J_{\mathbb{Q}}(\bar{f}, 2, \kappa)$, then since all of its components are nonnegative, we have from Equation 3.1.10 that

$$\begin{aligned} m[h_{(0,1,1)} + h_{(0,2,1)} + h_{(0,3,1)} + \ldots + h_{(0,m,1)}] \\ +(m-1)[h_{(0,1,2)} + h_{(0,2,2)} + h_{(0,3,2)} + \ldots + h_{(0,m,2)}] \\ +m[h_{(1,1,1)} + h_{(1,2,1)} + h_{(1,3,1)} + \ldots + h_{(1,m,1)}] \geq \kappa_0. \end{aligned}$$

Then by using Equation 3.1.11 in the above inequality, we arrive at

$$\begin{aligned} [h_{(0,1,1)} + h_{(0,2,1)} + h_{(0,3,1)} + \ldots + h_{(0,m,1)}] \geq \left(\frac{1}{m}\right)\kappa_0 - \left(\frac{m-1}{m}\right)\kappa_1 - \\ [h_{(1,1,1)} + h_{(1,2,1)} + h_{(1,3,1)} + \ldots + h_{(1,m,1)}] \end{aligned}$$

that is,

$$\sum_{\mu=1}^{m} h_{(0,\mu,1)} \geq \left(\frac{1}{m}\right)\kappa_0 - \left(\frac{m-1}{m}\right)\kappa_1 - \sum_{\mu=1}^{m} h_{(1,\mu,1)}.$$

Using the above inequality in Equation 3.1.12, we have

$$\begin{aligned} w(\kappa) &\geq \inf_{h \in J_{\mathbb{Q}}(\bar{f},2,\kappa)} \left\{ \left(\frac{1}{p}\right) \left[ \left(\frac{1}{m}\right)\kappa_0 - \left(\frac{m-1}{m}\right)\kappa_1 - \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right] + \left[ \kappa_1 + \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right] \right\} \\ &= \inf_{h \in J_{\mathbb{Q}}(\bar{f},2,\kappa)} \left\{ \left(\frac{1}{p}\right) \left[ \left(\frac{1}{m}\right)\kappa_0 - \left(\frac{m-1}{m}\right)\kappa_1 + p\kappa_1 \right] + \left(\frac{p-1}{p}\right) \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right\} \end{aligned}$$

Hence, we have

$$\begin{aligned} pw(\kappa) &= \inf_{h \in J_{\mathbb{Q}}(\bar{f},2,\kappa)} \left\{ \left[ \left(\frac{1}{m}\right)\kappa_0 - \left(\frac{m-1}{m}\right)\kappa_1 + p\kappa_1 \right] + (p-1) \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right\} \\ &\geq \left(\frac{1}{m}\right)\kappa_0 - \left[ p - \left(\frac{m-1}{m}\right) \right] \kappa_1 \\ &= w_2(\kappa). \end{aligned}$$

On the other hand, from Equation 3.1.12, we also have

$$\begin{aligned} & w(\kappa) \geq \kappa_1 \\ \implies & pw(\kappa) \geq p\kappa_1 = w_1(\kappa). \end{aligned}$$

Thus, we have

$$pw(\kappa) \geq \max\{w_1(\kappa), w_2(\kappa)\} = w_\Delta(\kappa).$$

□

From the above proposition along with Proposition 3.1.12, we observe that the diagram weight provides a quick easy estimate of the $p$-adic size of the coefficients $A(\kappa)$. Let us state this result for convenience.

**Proposition 3.1.20.** *For the case when $r = 2$, we have*

$$\operatorname{ord}_p A(\kappa) \geq \frac{w(\kappa)}{p-1} \geq \frac{w_\Delta(\kappa)}{p(p-1)}.$$

*Proof.* Combine the results of Proposition 3.1.12 and Proposition 3.1.19. □

We would naturally expect that the above result generalizes to

$$\operatorname{ord}_p A(\kappa) \geq \frac{w(\kappa)}{p-1} \geq \frac{w_\Delta(\kappa)}{p^{r-1}(p-1)}.$$

for all $r > 1$. This is indeed true for the case when $r = 3$ as we will see in the next subsection. Before we proceed to the $r = 3$ case, let us briefly discuss how the trace formula extends immediately to the $r = 2$ case.

**Trace Formula for the case when $r = 2$**

Let us summarize the results for the case when $r = 2$ as follows.

**Proposition 3.1.21.**

*Let $r = 2$ and let $F_{0,0}(x)$ be the power series associated to the polynomial $\bar{f}(\bar{x})$ defined (as described before) by*

$$F_{0,0}(x) = \prod_{\mu=1}^{m} \prod_{s=0}^{r-1} \prod_{k \in I(\mu,r,s)} \left[\theta_{r-d(k)-s}(a_{\mu,s}x^k)\right]^{c_{\mu,k}}.$$

*Then, on writing $F_{0,0}(x) = \sum_{\kappa \in \mathbb{Z}^r_{\geq 0}} A(\kappa)x^\kappa$, the coefficients $A(\kappa)$ satisfy*

$$\operatorname{ord}_p A(\kappa) \geq \frac{w_\Delta(\kappa)}{p^{r-1}(p-1)}$$

*where $w_\Delta(\kappa)$ is the diagrammatic weight of $\kappa$ described as before.*

The following results from the base case when $r = 1$ generalize gracefully in the $r = 2$ case as well. Set $M(f) := \mathbb{Z}^r_{\geq 0}$.

**Proposition 3.1.22.** *The diagrammatic weight function $w_\Delta$ satisfies the following properties:*

*(i) For each $\kappa \in M(f)$, $w_\Delta(\kappa)$ is the smallest nonnegative rational number $b$ such that $\kappa \in b\Delta(\bar{f}, 2) = \{v \in \mathbb{R}^r : bv \in \Delta(\bar{f}, 2)\}$ where $\Delta(\bar{f}, 2)$ is the level-2 $\Delta$-diagram of $\bar{f}$ as described before.*

*(ii) For $\alpha, \beta \in M(f)$, we have*

*(a) $w_\Delta(\alpha) = 0 \iff \alpha = 0$.*

*(b) $w_\Delta(c\alpha) = cw_\Delta(\alpha)$ if $c \geq 0$.*

*(c) $w_\Delta(\alpha + \beta) \leq w_\Delta(\alpha) + w_\Delta(\beta)$*

*(iii) There exists a positive integer $D$ such that for all $\kappa \in M(f)$, $w_\Delta(\kappa) \in \left(\frac{1}{D}\right)\mathbb{Z}$.*

*Proof.*

$(i)$ follows from an argument very similar to the analogous argument for the case when $r = 1$ given in the proof of Proposition 2.2.2. Then $(ii)$ follows from $(i)$. And $(iii)$ follows from an analogous argument as in Corollary 2.2.5. □

We are now in a position to construct certain $p$-adic Banach spaces associated to the polynomial $\bar{f}$ as in the $r = 1$ case. For each rational number $b \geq 0$, given a $p$-adic field, $K$, we may define the collection of formal power series,

$$B_{\bar{f}}(b, K) := \left\{ \sum_{\nu \in M(f)} A(\nu) x^{\nu} : A(\nu) \in K, \inf_{\nu \in M(f)} \{ \mathrm{ord}_p \, A(\nu) - w_{\Delta}(\nu) b \} > -\infty \right\}.$$

As before, we will omit the field $K$ in the notation $B_{\bar{f}}(b, K)$ and simply write $B_{\bar{f}}(b)$ once we have chosen the field, $K$. The choice of the field depends on the denominator of $b$ and the positive integer, $D$ in the previous proposition. By Dwork's theory, we observe that the $B_{\bar{f}}(b)$ are $p$-adic Banach spaces and we have

**Proposition 3.1.23.** *For rational numbers $b' > b \geq 0$, we have that the inclusion map $\mathbf{i} : B_{\bar{f}}(b') \hookrightarrow B_{\bar{f}}(b)$ is completely continuous.*

And we observe that the space $B_{\bar{f}}(b)$ can be expressed in terms of smaller subspaces, $B_{\bar{f}}(b, c)$ for real numbers $c$ as follows. Define

$$B_{\bar{f}}(b, c) := \left\{ \sum_{\nu \in M(f)} A(\nu) x^{\nu} : A(\nu) \in K, \mathrm{ord}_p \, A(\nu) \geq w_{\Delta}(\nu) b + c \right\}$$

so that $B_{\bar{f}}(b) = \bigcup_{c \in \mathbb{R}} B_{\bar{f}}(b, c)$. Then the following lemma (analogous to Lemma 2.2.7) holds.

**Lemma 3.1.24.** *Let $b$ be a nonnegative rational number and let $c, c'$ be real numbers. Then the following assertions hold.*

1. $B_{\bar{f}}(b, c) B_{\bar{f}}(b, c') \subset B_{\bar{f}}(b, c + c')$
2. *If $\xi(x) \in B_{\bar{f}}(b, c)$, then $\xi(x^p) \in B_{\bar{f}}(b/p, c)$*
3. *If rational numbers $b' > b > 0$, then $B_{\bar{f}}(b', c) \subset B_{\bar{f}}(b, c)$*

**Corollary 3.1.25.** *The series $F_{0,0}(x) \in B_{\bar{f}}\left( \dfrac{1}{p^{r-1}(p-1)}, 0 \right) \subset B_{\bar{f}}\left( \dfrac{1}{p^{r-1}(p-1)} \right)$.*

*Proof.* It follows from Proposition 3.1.21. □

Now let $\sigma$ denote the *Frobenius* generator of $Gal(\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r}))$. Then for any Laurent series, $F(x) = \sum_{\nu} A(\nu)x^{\nu} \in \mathbb{Q}_q(\zeta_p)\left((x_1, x_2..., x_n)\right)$, we can define the element obtained by the action of $\sigma^i$ on its coefficients as $F^{\sigma^i}(x) := \sum_{\nu} \sigma^i(A(\nu))x^{\nu}$ for $i = 0, 1, 2, ..., (a-1)$. Then we have the following corollary.

**Corollary 3.1.26.**

*(a) For each $i = 0, 1, ..., l-1$ and $j = 0, 1, ..., a-1$, the series $F_{i,j}(x) = F_{0,0}^{\sigma^j}(x^{p^{ia+j}}) \in B_{\bar{f}}\left(\frac{1}{p^{ia+j}p^{r-1}(p-1)}, 0\right) \subset B_{\bar{f}}\left(\frac{1}{p^{ia+j}p^{r-1}(p-1)}\right)$.*

*(b) The series $G(x) := \prod_{i=0}^{l-1}\prod_{j=0}^{a-1} F_{i,j}(x) \in B_{\bar{f}}\left(\frac{p}{q^l p^{r-1}(p-1)}, 0\right) \subset B_{\bar{f}}\left(\frac{p}{q^l p^{r-1}(p-1)}\right)$.*

*Proof.* First we recall that

$$\begin{aligned}
F_{i,j}(x) &= \prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\ 0\le s\le r-1\\ d(k)+s=u}}\left[\theta_{r-u}(a_{\mu,s}^{p^j}x^{kp^{ia+j}})\right]^{c_{\mu,k}}\\
&= \prod_{\mu=1}^{m}\prod_{s=0}^{r-1}\prod_{k\in I(\mu,r,s)}\left[\theta_{r-d(k)-s}(a_{\mu,s}^{p^j}x^{kp^{ia+j}})\right]^{c_{\mu,k}}\\
&= \prod_{\mu=1}^{m}\prod_{s=0}^{r-1}\prod_{k\in I(\mu,r,s)}\left[\theta_{r-d(k)-s}(\sigma^j(a_{\mu,s})x^{kp^{ia+j}})\right]^{c_{\mu,k}}\\
&= F_{0,0}^{\sigma^j}(x^{p^{ia+j}}).
\end{aligned}$$

Then it is clear from the above lemma and from the fact that $\operatorname{ord}_p \sigma^j(a_{\mu,s}) = \operatorname{ord}_p a_{\mu,s}$, that $F_{i,j}(x) \in B_{\bar{f}}\left(\frac{1}{p^{ia+j}p^{r-1}(p-1)}, 0\right) \subset B_{\bar{f}}\left(\frac{1}{p^{ia+j}p^{r-1}(p-1)}\right)$. Part $(b)$ follows from part $(a)$ and applying the lemma again. □

We now see that Dwork's Trace Formula extends naturally to this case when $r = 2$ with the $\Delta$-diagrammatic weight function $w_{\Delta}$.

### 3.1.4 The case when $r = 3$

We now have that $s$ runs from 0 through 2 and for each $\mu = 1, 2, ..., m$, we have $I(\mu, 3, 0) = \{(\mu, 0, 0), (\mu-1, 1, 0), (\mu-1, 0, 1), (\mu-2, 2, 0)\}$ and then $I(\mu, 3, 1) = \{(\mu, 0, 0), (\mu-1, 1, 0)\}$ and then $I(\mu, 3, 2) = \{(\mu, 0, 0)\}$. Then, for example, when $m = 4$, recall that the matrix $K(\bar{f}, 3)$ is given by Lemma 3.1.10:

$$K(\bar{f}, 3) = \left[ K_0(\bar{f}, 3) \,\middle\|\, K_1(\bar{f}, 3) \,\middle\|\, K_2(\bar{f}, 3) \right]$$

where

$$K_0(\bar{f}, 3) = \left[\begin{array}{ccc|cccc|cccc|cccc} 1 & 0 & 0 & 2 & 1 & 1 & 0 & 3 & 2 & 2 & 1 & 4 & 3 & 3 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}\right],$$

$$K_1(\bar{f}, 3) = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 2 & 1 & 3 & 2 & 4 & 3 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right], \text{ and}$$

$$K_2(\bar{f}, 3) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

That is,

$$K(\bar{f}, 3) = \left[\begin{array}{ccc|cccc|cccc|cccc||cc|cc|cc|cc||cccc} 1 & 0 & 0 & 2 & 1 & 1 & 0 & 3 & 2 & 2 & 1 & 4 & 3 & 3 & 2 & 1 & 0 & 2 & 1 & 3 & 2 & 4 & 3 & 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

where the first (leftmost) big block (demarcated by ||) corresponds to $s = 0$ and the next big block corresponds to $s = 1$ and the last big block corresponds to $s = 2$.

For a general $m$, the system of equations

$$K(\bar{f}, r) \cdot h = \kappa$$

read as follows.

$$
\begin{aligned}
&[h_{(0,1,1)} + 2h_{(0,2,1)} + 3h_{(0,3,1)} + \ldots + mh_{(0,m,1)}] \\
+&[0 + h_{(0,2,2)} + 2h_{(0,3,2)} + \ldots + (m-1)h_{(0,m,2)}] \\
+&[0 + h_{(0,2,3)} + 2h_{(0,3,3)} + \ldots + (m-1)h_{(0,m,3)}] \\
+&[0 + 0 + h_{(0,2,4)} + \ldots + (m-2)h_{(0,m,4)}] \\
+&[h_{(1,1,1)} + 2h_{(1,2,1)} + 3h_{(1,3,1)} + \ldots + mh_{(1,m,1)}] \\
+&[0 + h_{(1,1,2)} + 2h_{(1,2,2)} + \ldots + (m-1)h_{(1,m,2)}] \\
+&[h_{(2,1,1)} + 2h_{(2,2,1)} + 3h_{(2,3,1)} + \ldots + mh_{(2,m,1)}] = \kappa_0 \qquad (3.1.13) \\
&[h_{(0,1,2)} + h_{(0,2,2)} + \ldots + h_{(0,m,2)}] \\
+&[0 + 2h_{(0,2,4)} + \ldots + 2h_{(0,m,4)}] \\
+&[h_{(1,1,2)} + h_{(1,2,2)} + \ldots + h_{(1,m,2)}] = \kappa_1 \qquad (3.1.14) \\
&h_{(0,1,3)} + h_{(0,2,3)} + \ldots + h_{(0,m,3)} = \kappa_2 \qquad (3.1.15)
\end{aligned}
$$

For $m = 4$, the matrix $K_\Delta(\bar{f}, 3)$ is given by

$$
K_\Delta(\bar{f}, 3) = \left[ K_{\Delta,0}(\bar{f}, 3) \,\middle\|\, K_{\Delta,0}(\bar{f}, 3) \,\middle\|\, K_{\Delta,0}(\bar{f}, 3) \right]
$$

where

$$
K_{\Delta,0}(\bar{f}, 3) = \left[\begin{array}{ccc|cccc|cccc|cccc}
1 & 0 & 0 & 2 & \frac{1}{p} & \frac{1}{p^2} & 0 & 3 & \frac{2}{p} & \frac{2}{p^2} & \frac{1}{p^2} & 4 & \frac{3}{p} & \frac{3}{p^2} & \frac{2}{p^2} \\
0 & \frac{1}{p} & 0 & 0 & \frac{1}{p} & 0 & \frac{2}{p^2} & 0 & \frac{1}{p} & 0 & \frac{2}{p^2} & 0 & \frac{1}{p} & 0 & \frac{2}{p^2} \\
0 & 0 & \frac{1}{p^2} & 0 & 0 & \frac{1}{p^2} & 0 & 0 & 0 & \frac{1}{p^2} & 0 & 0 & 0 & \frac{1}{p^2} & 0
\end{array}\right],
$$

$$
K_{\Delta,1}(\bar{f}, 3) = \left[\begin{array}{cc|cc|cc|cc}
\frac{1}{p} & 0 & \frac{2}{p} & \frac{1}{p^2} & \frac{3}{p} & \frac{2}{p^2} & \frac{4}{p} & \frac{3}{p^2} \\
0 & \frac{1}{p^2} & 0 & \frac{1}{p^2} & 0 & \frac{1}{p^2} & 0 & \frac{1}{p^2} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right], \text{ and}
$$

$$
K_{\Delta,2}(\bar{f}, 3) = \begin{bmatrix}
\frac{1}{p^2} & \frac{2}{p^2} & \frac{3}{p^2} & \frac{4}{p^2} \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}.
$$

We now have propositions analogous to Proposition 3.1.16, Proposition 3.1.18, Proposition 3.1.19 and Proposition 3.1.20 stated below.

**Proposition 3.1.27.** *Let $m$ be a positive integer with $m > 1$. Let $S$ be the set of all columns of the matrix $K_\Delta(\bar{f}, 3)$ along with the zero vector. Then the convex hull of $S$ in $\mathbb{R}^3$ viewed as the 3-dimensional space defined by the $x_0, x_1$ and $x_2$ axes is simply the region bounded by the convex polytope with vertices $(m, 0, 0)$, $\left(\frac{m-1}{p}, \frac{1}{p}, 0\right)$, $\left(0, \frac{1}{p}, 0\right)$, $\left(0, 0, \frac{1}{p^2}\right)$, $\left(\frac{m-1}{p^2}, 0, \frac{1}{p^2}\right)$ and the origin $(0, 0, 0)$. And the faces of the polytope lie in the hyperplanes $x_0 = 0$, $x_1 = 0$, $x_2 = 0$, $w_1(x_0, x_1, x_2) = 1$ and $w_2(x_0, x_1, x_2) = 1$.*

*Proof.* It is not hard to see that all the points corresponding to the columns of the matrix $K_\Delta(\bar{f}, 3)$ lie on or within the specified convex polytope. First note that we need consider only the convex hull of the columns in $K_\Delta(\bar{f}, 3)$ for the $s = 0$ block. Also, within this first ($s = 0$) block, only the first and the last sub-blocks give the vertices (extreme points). It is important to note that since $p \geq 2$, we have that $\frac{2}{p^2} \leq \frac{1}{p}$. Finally, it is easily verified that the vertices $\left(\frac{m-1}{p}, \frac{1}{p}, 0\right)$, $\left(0, \frac{1}{p}, 0\right)$, $\left(0, 0, \frac{1}{p^2}\right)$ and $\left(\frac{m-1}{p^2}, 0, \frac{1}{p^2}\right)$ lie on the hyperplane defined by $w_1(x_0, x_1, x_2) = 1$ and that the vertices $(m, 0, 0)$, $\left(\frac{m-1}{p}, \frac{1}{p}, 0\right)$ and $\left(\frac{m-1}{p^2}, 0, \frac{1}{p^2}\right)$ lie on the hyperplane defined by $w_2(x_0, x_1, x_2) = 1$, and those along with the coordinate planes form the faces of the convex polytope. □

The convex polytope in the above proposition is called the **the level-3 Δ-diagram** of $\bar{f}$, and denote it by $\Delta(\bar{f}, 3)$. The figure below gives an example of such a level-3 Δ-diagram.

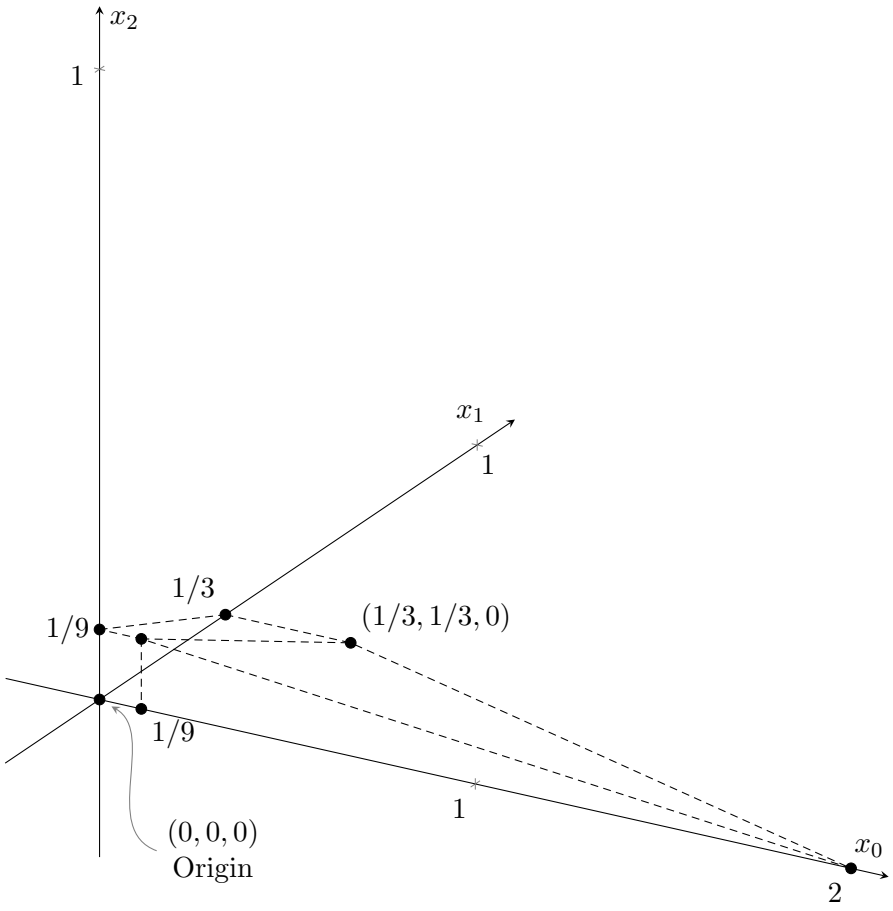



Figure 3.2: The level-3 $\Delta$-diagram corresponding to $\bar{f}$ with $m = 2$ and $p = 3$

By the arguments similar to those in Proposition 2.2.2, one can show the following result.

**Proposition 3.1.28.** *For $y = (y_0, y_1, y_2) \in \mathbb{Z}^3_{\geq 0}$, $w_\Delta(y)$ is the smallest nonnegative rational number, $b$ such that the convex set $b\Delta(\bar{f}, 3) := \{b\alpha : \alpha \in \Delta(\bar{f}, 3)\}$ includes $y$.*

We then have the following proposition.

**Proposition 3.1.29.** *For $\kappa = (\kappa_0, \kappa_1, \kappa_2) \in \mathbb{Z}^3_{\geq 0}$, one has*

$$p^2 w(\kappa) \geq w_\Delta(\kappa)$$

The proof of this proposition is a little too tedious due to the large number of columns of

the matrix $K_\Delta(\bar{f}, 3)$ that gave rise to the three long equations 3.1.13, 3.1.14 and 3.1.15. Please see Appendix C for a complete proof of the proposition.

We now have

**Proposition 3.1.30.** *For the case when $r = 3$, we have*

$$\operatorname{ord}_p A(\kappa) \geq \frac{w(\kappa)}{p-1} \geq \frac{w_\Delta(\kappa)}{p^2(p-1)}.$$

*Proof.* Combine the results of Proposition 3.1.12 and Proposition 3.1.29. □

And thus, we have

$$\operatorname{ord}_p A(\kappa) \geq \frac{w(\kappa)}{p-1} \geq \frac{w_\Delta(\kappa)}{p^{r-1}(p-1)}.$$

$r = 2$ and $r = 3$.

The trace formula for the $r = 3$ case extends in a very similar manner, however, as we noted in Appendix C, the mathematics for proving the proposition analogous to Proposition 3.1.19 gets more tedious as $r$ gets larger than or equal to 3. Hence, we consider an alternate approach as described in the next subsection to derive the trace formula in the general case for $r > 1$.

### 3.1.5 Alternate Approach

The rudimentary approaches above lead us to the following alternate approach in estimating the $p$-adic size of the coefficients of the power series, and thus arriving at a trace formula for the general case, $r > 1$.

**Growth of Coefficients of the Power Series associated to $\bar{f}$**

Consider the polynomial $\bar{f}(\bar{x})$ in terms of *Teichmüller variables* $(x_j)_{0\leq j\leq r-1}$ whenever $\bar{x}$ is a variable taking values in $(\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l})$ as follows:

$$\begin{aligned}
\bar{f}(\bar{x}) &= \sum_{\mu=1}^{m} \bar{a}_\mu x^\mu \\
&= \sum_{\mu=1}^{m}\sum_{s=0}^{r-1} a_{\mu,s}p^s \left(\sum_{j=0}^{r-1} x_j p^j\right)^\mu \\
&= \sum_{\mu=1}^{m}\sum_{s=0}^{r-1} a_{\mu,s}p^s \sum_{k\in I(\mu,r)} c_{\mu,k}\left(\prod_{j=0}^{r-1} x_j^{k_j}\right) p^{d(k)} \\
&= \sum_{\mu=1}^{m}\sum_{k\in I(\mu,r)}\sum_{s=0}^{r-1} a_{\mu,s}c_{\mu,k}x^k p^{d(k)+s} \qquad (3.1.16)
\end{aligned}$$

for some integer coefficients $c_{\mu,k}$, where the variable $\bar{x}$ has its $p$-adic expansion in terms of Teichmüller variables $x_0, x_1, ..., x_{r-1}$ given by $\bar{x} = \sum_{j=0}^{r-1} x_j p^j$, and $\sum_{s=0}^{r-1} a_{\mu,s}p^s$ is the $p$-adic representation of the $\bar{a}_\mu$ in terms of Teichmüller digits, $a_{\mu,s}$.

Now, if $\bar{x} \in (\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l})$ and if we denote the vector of Teichmüller variables $(x_0, x_1, ..., x_{r-1})$ by $x$, then applying the character $\Theta_r \circ \tau(q,l,r)$ to $\bar{f}(\bar{x})$ we get

$$\begin{aligned}
\Theta_r \circ \tau(q,l,r)\left(\bar{f}(\bar{x})\right) &= \prod_{\mu=1}^{m}\prod_{k\in I(\mu,r)}\prod_{s=0}^{r-1}\left[\Theta_r \circ \tau(q,l,r)\left(a_{\mu,s}x^k p^{d(k)+s}\right)\right]^{c_{\mu,k}} \\
&= \prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\ 0\leq s\leq r-1\\ d(k)+s=u}}\left[\Theta_r \circ \tau(q,l,r)\left(a_{\mu,s}x^k p^u\right)\right]^{c_{\mu,k}} \\
&= \prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\ 0\leq s\leq r-1\\ d(k)+s=u}}\left[\prod_{j=0}^{al-1}\theta_{r-u}(a_{\mu,s}^{p^j}x^{kp^j})\right]^{c_{\mu,k}} \\
&= \prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\ 0\leq s\leq r-1\\ d(k)+s=u}}\left[\prod_{i=0}^{l-1}\prod_{j=0}^{a-1}\theta_{r-u}(a_{\mu,s}^{p^j}x^{kp^{ia+j}})\right]^{c_{\mu,k}}
\end{aligned}$$

$$= \prod_{i=0}^{l-1}\prod_{j=0}^{a-1}\prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\0\le s\le r-1\\d(k)+s=u}}\left[\theta_{r-u}(a_{\mu,s}^{p^j}x^{kp^{ia+j}})\right]^{c_{\mu,k}} \qquad (*)$$

where the third equality follows from the basic theory we established in the previous document and the fourth equality follows from the fact that $a_{\mu,s}^{q} = a_{\mu,s}$, and hence we have obtained an analogue of Proposition 2.1.21 in Chapter 2.

**Definition 3.1.31.** For each $i \in \{0, 1, ..., l-1\}$ and for each $j \in \{0, 1, ..., a-1\}$, we define

$$\boxed{F_{i,j}(x) := \prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\0\le s\le r-1\\d(k)+s=u}}\left[\theta_{r-u}(a_{\mu,s}^{p^j}x^{kp^{ia+j}})\right]^{c_{\mu,k}}} \qquad (3.1.17)$$

where $x = (x_0, x_1, ..., x_{r-1})$, the $a_{\mu,s}$ are the Teichmüller digits of the coefficients $\bar{a}_\mu$ as defined before and the $c_{\mu,k}$ are the integer coefficients obtained from the multinomial expansions as discussed before and $\mu$ runs over $Supp(\bar{f})$.

With the above definition we have

$$\Theta^{(r)} \circ \tau(q,l,r)\left(\bar{f}(\bar{x})\right) = \prod_{i=0}^{l-1}\prod_{j=0}^{a-1} F_{i,j}(x) \qquad (3.1.18)$$

Let us now analyze the growth of the coefficients of the basic series $F_{0,0}(x)$. In order to emphasize the degree, $m$ of the polynomial, $\bar{f}$ (which is useful in determining the weight functions) we incorporate that into the notation. Consider (as before)

$$F_{0,0}^{(m)}(x) := F_{0,0}(x) = \prod_{\mu=1}^{m}\prod_{u=0}^{r-1}\prod_{\substack{k\in I(\mu,r)\\0\le s\le r-1\\d(k)+s=u}}\left[\theta_{r-u}(a_{\mu,s}x^{k})\right]^{c_{\mu,k}}.$$

For fixed $(u, \mu, k, s)$ with $\boxed{u = d(k) + s}$, define $\boxed{F_{0,0}^{(u,\mu,k,s)}(x) := \left[\theta_{r-u}(a_{\mu,s}x^{k})\right]^{c_{\mu,k}}}$, so

that

$$\boxed{F_{0,0}^{(m)}(x) = \prod_{u=0}^{r-1} \prod_{\mu=1}^{m} \prod_{\substack{k \in I(\mu,r) \\ 0 \le s \le r-1 \\ d(k)+s=u}} F_{0,0}^{(u,\mu,k,s)}(x)}. \tag{3.1.19}$$

Then we have the following proposition.

**Proposition 3.1.32.**

$$F_{0,0}^{(u,\mu,k,s)}(x) = \sum_{h^{(k)}=0}^{\infty} B_{(u,\mu,s)}(k, h^{(k)}) x^{kh^{(k)}}$$

*where the coefficients* $B_{(u,\mu,s)}(k, h^{(k)})$ *satisfy*

$$\operatorname{ord}_p B_{(u,\mu,s)}(k, h^{(k)}) \ge \frac{h^{(k)}}{p^{r-1-d(k)-s}(p-1)} = \frac{h^{(k)}}{p^{r-1-u}(p-1)} \ge \frac{h^{(k)}}{p^{r-1-d(k)}(p-1)}.$$

*Proof.* We recall that the integer $c_{\mu,k}$ is simply the multinomial coefficient, $\binom{\mu}{k_0,k_1,\ldots,k_{r-1}}$. Then for some coefficients $b_h^{(r-d(k)-s)}$,

$$\begin{aligned} F_{0,0}^{(u,\mu,k,s)}(x) &= \left( \sum_{h=0}^{\infty} b_h^{(r-d(k)-s)} x^{kh} \right)^{c_{\mu,k}} \\ &= \prod_{j=0}^{c_{\mu,k}} \sum_{h_j=0}^{\infty} b_{h_j}^{(r-d(k)-s)} x^{kh_j} \\ &= \sum_{h^{(k)}=0}^{\infty} B_{(\mu,r,s)}(k, h^{(k)}) x^{kh^{(k)}} \end{aligned}$$

where

$$B_{(u,\mu,s)}(k, h^{(k)}) = \sum \prod_{j=1}^{c_{\mu,k}} b_{h_j}^{(r-d(k)-s)}$$

where the sum runs over $\mathbf{h} = (h_1, h_2, ..., h_{c_{\mu,k}}) \in \mathbb{Z}_{\ge 0}^{c_{\mu,k}}$ such that $\sum_{j=1}^{c_{\mu,k}} h_j = h^{(k)}$. And we have

$$\operatorname{ord}_p B_{(u,\mu,s)}(k, h^{(k)}) \ge \inf \left\{ \sum_{j=1}^{c_{\mu,k}} \operatorname{ord}_p b_{h_j}^{(r-d(k)-s)} : \sum_{j=1}^{c_{\mu,k}} h_j = h^{(k)} \right\}$$

$$\geq \sum_{j=1}^{c_{\mu,k}} \frac{h_j}{p^{r-d(k)-s-1}(p-1)}$$
$$= \frac{h^{(k)}}{p^{r-d(k)-s-1}(p-1)}$$

by the $p$-adic analytic properties of the function $\theta_{r-d(k)-s}(t)$ established earlier. $\square$

### The two ways of looking at $F_{0,0}^{(m)}(x)$

Let us note carefully the two ways of looking at the power series, $F_{0,0}^{(m)}(x)$. The first way is useful in getting tighter estimates based on an algebraically defined weight function (what we called an "intuitive" weight function) that we considered in the previous subsections in our "rudimentary" approach. We also recall that we defined the $\Delta$-diagrammatic weight function that bounded the "intuitive" weight function. We will see that the second way of looking at it using the new approach based on Equation 3.1.19 is useful in obtaining estimates on the size of its coefficients using a convenient diagrammatic weight function more easily without going through the computational trouble that we encountered in the rudimentary approach.

The first way is to write the product expressing $F_{(0,0)}^{(m)}(x)$ as we originally looked at in the first rudimentary approach:

$$F_{0,0}^{(m)}(x) = \prod_{\mu=1}^{m} \prod_{s=0}^{r-1} \prod_{k \in I(\mu,r,s)} \left[\theta_{r-d(k)-s}(a_{\mu,s}x^k)\right]^{c_{\mu,k}}.$$

where $I(\mu, r, s)$ is the subset of $I(\mu, r)$ consisting of those monomial vectors $k$ for which $d(k) < r - s$. Now for fixed $(\mu, s)$ let

$$F_{0,0}^{(\mu,r,s)}(x) := \prod_{k \in I(\mu,r,s)} \left[\theta_{r-d(k)-s}(a_{\mu,s}x^k)\right]^{c_{\mu,k}} \tag{3.1.20}$$

Recall that with the first approach, we proved Proposition 3.1.7 which stated that

$$F_{0,0}^{(\mu,r,s)}(x) = \prod_{k \in I(\mu,r,s)} \sum_{h^{(k)}=0}^{\infty} B_{(\mu,r,s)}(k, h^{(k)}) x^{kh^{(k)}}$$

where the coefficients $B_{(\mu,r,s)}(k,h^{(k)})$ satisfy

$$\boxed{\operatorname{ord}_p B_{(\mu,r,s)}(k,h^{(k)}) \geq \frac{h^{(k)}}{p^{r-d(k)-s-1}(p-1)} \geq \frac{h^{(k)}}{p^{r-d(k)-1}(p-1)}}.$$

Here is the second way using our new approach (notice the change in the order in which the products are taken in expressing $F^{(m)}_{(0,0)}(x)$). Following the description above, we have

$$\begin{aligned} F^{(m)}_{0,0}(x) &= \prod_{u=0}^{r-1}\prod_{\mu=1}^{m}\prod_{\substack{k\in I(\mu,r)\\0\leq s\leq r-1\\d(k)+s=u}} F^{(u,\mu,k,s)}_{0,0}(x) \\ &= \prod_{u=0}^{r-1}\prod_{\mu=1}^{m}\prod_{\substack{k\in I(\mu,r)\\0\leq s\leq r-1\\d(k)+s=u}}\sum_{h^{(k)}=0}^{\infty} B_{(u,\mu,s)}(k,h^{(k)})x^{kh^{(k)}} \end{aligned}$$

for some coefficients $B_{(u,\mu,s)}(k,h^{(k)})$ satisfying $\boxed{\operatorname{ord}_p B_{(u,\mu,s)}(k,h^{(k)}) \geq \frac{h^{(k)}}{p^{r-d(k)-s-1}(p-1)}}$ by Proposition 3.1.32.

### The Λ-diagram Weight Function

Let us now develop a diagrammatic weight function.

**Definition 3.1.33.** Recall that for each $s = 0, 1, 2, ..., r-1$, $I(\mu,r,s)$ is the subset of $I(\mu,r)$ consisting of those monomial vectors $k$ for which $d(k) < r-s$. Let $\bar{\rho}(\mu,r,s)$ be the cardinality of $I(\mu,r,s)$. The members of $I(\mu,r,0)$ are the same as the members of $I(\mu,r)$ which are obtained by applying Lemma 3.1.1. We may arrange these members in a total order dictated by the lexicographic ordering of the corresponding partitions of integers as per Proposition 3.1.4. Then the sets $I(\mu,r,1), I(\mu,r,2), ...$ are simply truncations of the set $I(\mu,r,0)$. We may put them all together in a matrix $K(\mu,r) := [I(\mu,r,0)\ \ I(\mu,r,1)\ \ ...\ \ I(\mu,r,r-1)]$ that has $r$ rows and $\sum_{s=0}^{r-1}\bar{\rho}(\mu,r,s)$ columns.

**Example 3.1.34.** Let $r = 3$ and let $\mu \geq 2$. Then

$$K(\mu, r) = \left[\begin{array}{cccc|cc|c} \mu & \mu-1 & \mu-1 & \mu-2 & \mu & \mu-1 & \mu \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right]$$

Observe that the matrix is divided into three blocks of columns where the first block corresponds to $s = 0$, the second one corresponds to $s = 1$ and the last one to $s = 2$.

**Example 3.1.35.** Let $r = 3$ and let $\mu = 1$. Then

$$K(\mu, r) = \left[\begin{array}{ccc|cc|c} \mu & \mu-1 & \mu-1 & \mu & \mu-1 & \mu \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right]$$

Observe that when $\mu = 1$, $\mu - 2$ is negative, and therefore we have only 3 columns in the $s = 0$ block in this case.

Let us now modify the matrix $K(\mu, r)$ slightly in order to accommodate the effect of $d(k)$ and $s$ for each column $k$ in the matrix. We define the matrix $\underline{K}(\mu, r)$ as follows.

**Definition 3.1.36.** Replace each column $k$ in the matrix $K(\mu, r)$ with the column $p^{r-1-d(k)-s}k$. Recall that $d(k) = \sum_{j=0}^{r-1} jk_j$ and that $s$ corresponds to the block in which the column is in. We thus obtain the matrix $\underline{K}(\mu, r)$. The columns of this matrix are denoted by $\underline{k}$ so that $\underline{k} = p^{r-1-d(k)-s}k$ where $k$ is the corresponding column in $K(\mu, r)$.

**Example 3.1.37.** Let $r = 3$ and let $\mu \geq 2$. Recall that

$$K(\mu, r) = \left[\begin{array}{cccc|cc|c} \mu & \mu-1 & \mu-1 & \mu-2 & \mu & \mu-1 & \mu \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right]$$

and that the matrix is divided into three blocks of columns where the first block corresponds to $s = 0$, the second one corresponds to $s = 1$ and the last one to $s = 2$.

Then,

$$\underline{K}(\mu,r)=\left[\begin{array}{cccc|cc|c} p^2\mu & p(\mu-1) & (\mu-1) & (\mu-2) & p\mu & (\mu-1) & \mu \\ 0 & p & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right].$$

**Example 3.1.38.** Let $r=3$ and let $\mu=1$. Recall that

$$K(\mu,r)=\left[\begin{array}{ccc|cc|c} \mu & \mu-1 & \mu-1 & \mu & \mu-1 & \mu \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right].$$

Then

$$\underline{K}(\mu,r)=\left[\begin{array}{ccc|cc|c} p^2\mu & p(\mu-1) & (\mu-1) & p\mu & (\mu-1) & \mu \\ 0 & p & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right].$$

Let us now define a *diagrammatic* weight function that is almost the same as the previously defined diagrammatic weight function, except for a factor of a $p$ power (This slight modification is helpful in proving Bombieri-Adolphson-Sperber's degree estimates later on in Chapter 5).

**Definition 3.1.39.** The **level-$r$ $\Lambda$-diagram** (or simply the **level-$r$ diagram**) corresponding to the polynomial $\bar{f}$ is defined as the convex closure (hull) of the columns of the matrices $\underline{K}(\mu,r)$ as $\mu$ runs over $Supp(\bar{f})$ along with the origin when looking at them as vectors in $\mathbb{R}^r$. We denote this by $\Lambda(\bar{f},r)$, and we write $\Lambda(\bar{f},r)=Conv\left(\{\underline{k}:\underline{k}\in\underline{K}(\mu,r):\mu\in Supp(\bar{f})\}\cup\{\mathbf{0}\}\right)$.

The figures below give some examples of such level-$r$ diagrams for $\bar{f}$ being a polynomial of degree $m$. For simplicity, we assume that $Supp(\bar{f})=\{1,2,...,m\}$.

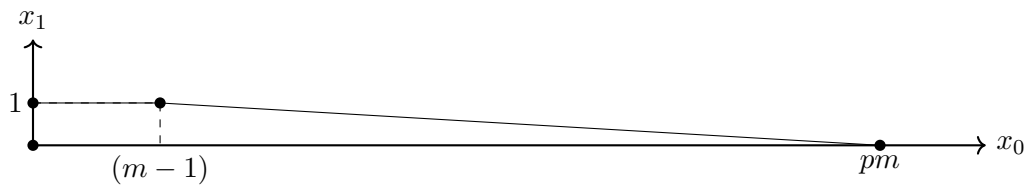



Figure 3.3: The level-2 Λ-diagram corresponding to $\bar{f}$ with $m = 4$ and $p = 5$

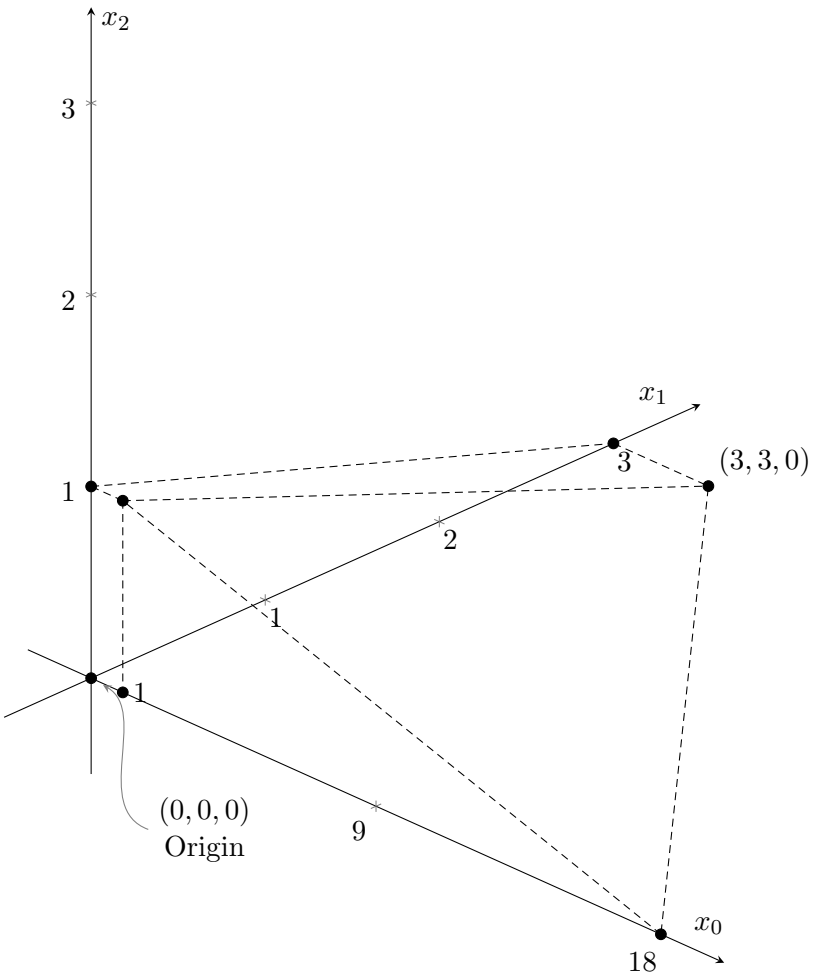



Figure 3.4: The level-3 Λ-diagram corresponding to $\bar{f}$ with $m = 2$ and $p = 3$

**Definition 3.1.40.** Let $f = f(x)$ be the $r$-expansion of $\bar{f}(\bar{x})$. Let $Cone(f)$ be the union in $\mathbb{R}^r$ of all the rays from the origin passing through all the points in $\Lambda(\bar{f}, r)$. Let

$M(f) := Cone(f) \cap \mathbb{Z}^r$.

**Definition 3.1.41.** For convenience, it is useful to define the submatrices of $\underline{K}(\mu, r)$ that consist only of the columns that correspond respectively to $s = 0$, $s = 1$, ..., $s = (r-1)$ and let us denote these by $\underline{K}_s(\mu, r)$ for each $s = 0, 1, ..., (r-1)$.

It is easy to see that the following proposition holds by the definition of the matrix $\underline{K}(\mu, r)$.

**Proposition 3.1.42.** *From the above definitions, we have*

$$\Lambda(\bar{f}, r) = Conv\left(\{\underline{k} : \underline{k} \in \underline{K}_0(\mu, r), \mu \in Supp(\bar{f})\} \cup \{\mathbf{0}\}\right)$$

*Proof.* The columns of $\underline{K}_s(\mu, r)$ for $s \geq 1$ are simply convex combinations of a column of $\underline{K}_0(\mu, r)$ along with the origin. □

By the above proposition, we observe that only the columns of $\underline{K}_0(\mu, r)$ as $\mu$ runs over $Supp(\bar{f})$ matter for the $\Lambda$-diagram.

**Definition 3.1.43.** For $y = (y_1, y_2, ..., y_{r-1}) \in M(f)$, the **level $r$ $\Lambda$-diagram weight** (or simply the diagram weight when there is no confusion about which diagram we refer to), $w_\Lambda(y)$ is defined as the smallest nonnegative rational number $b$ such that $y \in b\Lambda(\bar{f}, r) := \{v \in \mathbb{R}^r : bv \in \Lambda(\bar{f}, r)\}$.

**Proposition 3.1.44.** *The level $r$ $\Lambda$-diagram weight function $w_\Lambda$ satisfies the following properties:*

*For $\alpha, \beta \in M(f)$, we have*

*(i)* $w_\Lambda(\alpha) = 0 \iff \alpha = 0$.

*(ii)* $w_\Lambda(c\alpha) = cw_\Lambda(\alpha)$ *if* $c \geq 0$.

*(iii)* $w_\Lambda(\alpha + \beta) \leq w_\Lambda(\alpha) + w_\Lambda(\beta)$

*(iv) There exists a positive integer $D$ such that for all $\kappa \in M(f)$, $w_\Lambda(\kappa) \in \left(\frac{1}{D}\right)\mathbb{Z}$.*

*Proof.*
$(i), (ii)$ and $(iii)$ follows easily from the definition of the $\Lambda$-diagram as a convex closure. And $(iv)$ follows from an analogous argument as in Corollary 2.2.5. $\square$

Let us now define an analytical weight function and we will show that this analytical weight function coincides with the $\Lambda$-diagrammatic weight function for the single variable case.

**Definition 3.1.45.** For $y = (y_0, y_1, ..., y_{r-1}) \in M(f)$, define the following:

$$w_1(y) := \left(\frac{1}{p^{r-1}}\right)\left[py_1 + p^2y_2 + ... + p^{r-1}y_{r-1}\right] = \frac{1}{p^{r-1}}\sum_{j=1}^{r-1} p^j y_j.$$

$$w_2(y) := \left(\frac{1}{p^{r-1}}\right)\left[\left(\frac{1}{m}\right)y_0 + \left(p - \frac{m-1}{m}\right)y_1 + ... + \left(p^{r-1} - \frac{m-1}{m}\right)y_{r-1}\right]$$
$$= \left(\frac{1}{p^{r-1}}\right)\sum_{j=0}^{r-1}\left(p^j - \frac{m-1}{m}\right)y_j.$$

$$\bar{w}_\Lambda(y) := \max\{w_1(y), w_2(y)\}.$$

We say that $\bar{w}_\Lambda(y)$ is the **analytical expression of the $\Lambda$-diagram weight** of $y$.

Let us now show how this analytical expression coincides with the $\Lambda$-diagram weight defined before.

**Lemma 3.1.46.** *Let $r \geq 2$, $1 \leq \mu \leq m$ and let $k \in I(\mu, r)$. Suppose that $w_1(k) \leq 1$ and that $w_2(k) \leq 1$. Let $k' \in I(\mu, r+1)$ be a monomial derived from $k$ as per Lemma 3.1.1. Let $w_1'$ and $w_2'$ denote the extension of the linear forms $w_1$ and $w_2$ to dimension, $r+1$. Then $w_1'(k') \leq 1$ and $w_2'(k') \leq 1$.*

*Proof.* Writing $k = (k_0, k_1, ..., k_{r-1})$, we have that $k'$ has the form $k' = (k_0, k_1, ..., k_i - 1, k_{i+1} + 1, k_{i+2}..., k_{r-1}, 0)$ for some $i = 0, 1, ..., r-1$. And we also have that $\sum_{i=0}^{r-1} k_i = \mu$. Then we have

$$
\begin{aligned}
w_1'(k') &= w_1'\left(k_0, k_1, ..., k_{i-1}, k_i - 1, k_{i+1} + 1, k_{i+2}, ..., k_{r-1}, 0\right) \\
&= \left(\frac{1}{p^r}\right)\left[pk_1 + p^2k_2 + ... + p^{i-1}k_{i-1} + p^i(k_i - 1) + p^{i+1}(k_{i+1} + 1) + p^{i+2}k_{i+2} + ... \right. \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \left. + p^{r-1}k_{r-1}\right] \\
&= \left(\frac{1}{p}\right)\left(\frac{1}{p^{r-1}}\right)\left[\left(pk_1 + p^2k_2 + ... + p^{r-1}k_{r-1}\right) + \left(p^{i+1} - p^i\right)\right] \\
&= \left(\frac{1}{p}\right)\left[w_1(k) + \left(\frac{1}{p^{r-1}}\right)\left(p^{i+1} - p^i\right)\right] \\
&\leq \left(\frac{1}{p}\right)\left[1 + \left(\frac{p^i(p-1)}{p^{r-1}}\right)\right] \\
&\leq \frac{p^{r-1} + p^{r-1}(p-1)}{p^r} = 1.
\end{aligned}
$$

Similarly, we have

$$
\begin{aligned}
w_2'(k') &= w_2'\left(k_0, k_1, ..., k_{i-1}, k_i - 1, k_{i+1} + 1, k_{i+2}, ..., k_{r-1}, 0\right) \\
&= \left(\frac{1}{p^r}\right)\left(\left(\frac{1}{m}\right)k_0 + \left(p - \frac{m-1}{m}\right)k_1 + ... + \left(p^i - \frac{m-1}{m}\right)(k_i - 1)\right. \\
&\qquad + \left(p^{i+1} - \frac{m-1}{m}\right)(k_{i+1} + 1) + \left(p^{i+2} - \frac{m-1}{m}\right)k_{i+2} + ... \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \left. + \left(p^{r-1} - \frac{m-1}{m}\right)k_{r-1}\right) \\
&= \left(\frac{1}{p}\right)\left(\frac{1}{p^{r-1}}\right)\left[\left(\left(\frac{1}{m}\right)k_0 + \left(p - \frac{m-1}{m}\right)k_1 + ... \right.\right. \\
&\qquad\qquad\qquad\qquad\qquad\qquad \left.\left. + \left(p^{r-1} - \frac{m-1}{m}\right)k_{r-1}\right) + \left(p^{i+1} - p^i\right)\right] \\
&= \left(\frac{1}{p}\right)\left[w_2(k) + \left(\frac{1}{p^{r-1}}\right)\left(p^{i+1} - p^i\right)\right] \\
&\leq \left(\frac{1}{p}\right)\left[1 + \left(\frac{p^i(p-1)}{p^{r-1}}\right)\right] \\
&\leq \frac{p^{r-1} + p^{r-1}(p-1)}{p^r} = 1.
\end{aligned}
$$

□

**Proposition 3.1.47.** *Let $y \in M(f)$. Then*

$$w_\Lambda(y) = \bar{w}_\Lambda(y).$$

*Proof.* Let $d$ be the dimension of $\Lambda(\bar{f}, r)$. (Here, of course, $d = r$). The main argument in the proof is to establish that there are only two $(d-1)$-faces of the polyhedron, $\Lambda(\bar{f}, r)$ that do not pass through the origin, and they lie on the hyperplanes defined my the equations $w_1(x) = 1$ and $w_2(x) = 1$. Once this is established, the result follows by the same argument as in Proposition 2.2.2.

The claimed statement is easily seen to be true in the case when $r = 2$ by a straightforward calculation. For $r \geq 3$, first note that if $w_1(y) \leq 1$ and $w_2(y) \leq 1$ at level $r-1$, then clearly $w_1(y, 0) \leq 1$ and $w_2(y, 0) \leq 1$ (where $w_1$ and $w_2$ also denote the extensions of the linear forms $w_1$ and $w_2$ to level $r$) as well at level $r$. Also, Lemma 3.1.46 proves that the (new) derived monomials from level $(r-1)$ satisfy the inequalities $w_1(x) \leq 1$ and $w_2(x) \leq 1$. Also, it is easily seen that the lattice points corresponding to the monomial vectors $(m, 0, 0, ..., 0)$ and $(m-1, 1, 0, 0, ..., 0)$ (which are present in $I(m, r)$ for every $r \geq 3$), namely, $(p^{r-1}m, 0, 0, ..., 0)$ and $(p^{r-2}(m-1), p^{r-2}, 0, 0, ..., 0)$ precisely lie on the hyperplanes $w_2(x) = 1$ and $w_1(x) = 1$ respectively. Thus there is at least one point that lie *on* each of the hyperplanes $w_2(x) = 1$ and $w_1(x) = 1$.

Thus, we deduce that

$$w_\Lambda(y) = \bar{w}_\Lambda(y).$$

□

Now, from Proposition 3.1.32, we immediately deduce the following result.

**Proposition 3.1.48.** *For fixed $(u, \mu, k, s)$ with $u \in \{0, 1, ..., r-1\}$, $\mu \in \{1, 2, ..., m\}$, $k \in I(\mu, r)$ and $u = d(k) + s$, when the power series, $F_{(u,\mu,k,s)}(x)$ is written out as $\sum_v A_v x^v$, then the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1}.$$

*Proof.* From Proposition 3.1.32, we have that

$$F_{(u,\mu,k,s)}(x) = \sum_{h^{(k)}=0}^{\infty} B(k, h^{(k)}) x^{kh^{(k)}}$$

where the coefficients $B(k, h^{(k)})$ satisfy

$$\operatorname{ord}_p B(k, h^{(k)}) \geq \frac{h^{(k)}}{p^{r-1-u}(p-1)}.$$

So, for $v = kh^{(k)}$, we have

$$\begin{aligned} & \operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1} \\ \iff & \operatorname{ord}_p A_v \geq \frac{w_\Lambda(kh^{(k)})}{p-1} \\ \iff & \operatorname{ord}_p A_v \geq \frac{h^{(k)} w_\Lambda(k)}{p-1} \end{aligned}$$

and

$$\operatorname{ord}_p A_v \geq \frac{h^{(k)}}{p^{r-1-u}(p-1)}.$$

Hence it suffices to prove that

$$\frac{1}{p^{r-1-u}} \geq w_\Lambda(k) \iff w_\Lambda(p^{r-1-d(k)-s}k) \leq 1.$$

But the last inequality is easily seen to be true by observing that $\underline{k} := p^{r-1-d(k)-s}k$ is simply a column in the matrix $\underline{K}(\mu, r)$. □

The following lemma helps us to prove the important application of the above proposition.

**Lemma 3.1.49.** *Let $N$ be a positive integer, $K$ be a positive constant and for each $i = 1, 2, ..., N$, let $H_i(x) = \sum_{j \in Supp(H_i)} C_{i,j} x^j$ be a power series in several variables with the $j$ being nonnegative vectors and the coefficients belonging to $\mathbb{C}_p$ are such that for all $i, j$,*

$$\operatorname{ord}_p C_{i,j} \geq K w_\Lambda(j).$$

*Let $H(x) = \prod_{i=1}^{N} H_i(x)$. Then when $H(x)$ is written out as $\sum_v A_v x^v$, the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq K w_\Lambda(v)$$

*Proof.* Writing out the product, we have

$$\begin{aligned}\sum_v A_v x^v = H(x) &= \prod_{i=1}^N H_i(x) \\ &= \prod_{i=1}^N \sum_j C_{i,j} x^j \\ &= \sum_v \sum_{j_1+j_2+\ldots+j_N=v} \left( \prod_{i=1}^N C_{i,j_i} \right) x^v\end{aligned}$$

Thus, the coefficients $A_v$ satisfy

$$\begin{aligned}\operatorname{ord}_p A_v &\geq \inf \left\{ \sum_{i=1}^N \operatorname{ord}_p C_{i,j_i} : j_1 + j_2 + \ldots + j_N = v \right\} \\ &\geq \sum_{i=1}^N K w_\Lambda(j_i) \\ &\geq K w_\Lambda \left( \sum_{i=1}^N j_i \right) \\ &= K w_\Lambda(v).\end{aligned}$$

□

We finally have

**Proposition 3.1.50.** *When the power series, $F^{(m)}_{(0,0)}(x)$ is written out as $\sum_v A_v x^v$, the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1}$$

*Proof.* From the above proposition, we have that if $F^{(u,\mu,k,s)}_{0,0}(x) = \sum_\ell C_\ell x^\ell$, then the coefficients $C_\ell$ satisfy

$$\operatorname{ord}_p C_\ell \geq \frac{w_\Lambda(\ell)}{p-1}.$$

Then for

$$\sum_v A_v x^v = F_{0,0}^{(m)}(x) = \prod_{u=0}^{r-1} \prod_{\mu=1}^{m} \prod_{\substack{k \in I(\mu,r) \\ 0 \le s \le r-1 \\ d(k)+s=u}} F_{0,0}^{(u,\mu,k,s)}(x)$$

the coefficients $A_v$ satisfy

$$\operatorname{ord}_p A_v \ge \frac{w_\Lambda(v)}{p-1}$$

by the preceding lemma. □

From Proposition 3.1.50, it is easily seen that Dwork's Trace Formula extends naturally to the general case with $r > 1$, with respect to the $\Lambda$-diagram weight for the single variable case.

## 3.2 The Multivariable Case

Let us now consider the multivariable case and generalize the previous theory for the single variable case. Let $\{\bar{x}_i : i = 1, 2, ..., n\}$ be a set of $n$ variables and let $\boldsymbol{\mu} = (\mu_1, \mu_2, ..., \mu_n)$ be a vector of nonnegative integers and let the symbol $\bar{\mathbf{x}}^{\boldsymbol{\mu}}$ denote $\bar{x}_1^{\mu_1}\bar{x}_2^{\mu_2}...\bar{x}_n^{\mu_n}$. Let $\bar{f}(\bar{\mathbf{x}}) \in (\mathbb{Z}_q/p^r\mathbb{Z}_q)[\bar{x}_1, \bar{x}_2, ..., \bar{x}_n]$ of degree $m$ written out as

$$\bar{f}(\bar{\mathbf{x}}) = \sum_{\boldsymbol{\mu} \in Supp(\bar{f})} a_{\boldsymbol{\mu}} \bar{\mathbf{x}}^{\boldsymbol{\mu}}$$

so that for all $\boldsymbol{\mu} \in Supp(\bar{f})$, $|\boldsymbol{\mu}| := \mu_1 + \mu_2 + ...\mu_n \leq m$ and there is some $\boldsymbol{\mu} \in Supp(\bar{f})$ such that $|\boldsymbol{\mu}| = m$.

Then the $r$**-expansion** of $\bar{f}(\bar{\mathbf{x}})$ in terms of the *Teichmüller variables* $(x_{i,j})_{\substack{i=1,2,...,n \\ j=0,1,...,r-1}}$ is given by

$$\begin{aligned}
\bar{f}(\bar{\mathbf{x}}) &= \sum_{\boldsymbol{\mu} \in Supp(\bar{f})} a_{\boldsymbol{\mu}} \bar{\mathbf{x}}^{\boldsymbol{\mu}} \\
&= \sum_{\boldsymbol{\mu} \in Supp(\bar{f})} \left( \sum_{s=0}^{r-1} a_{\boldsymbol{\mu},s} p^s \right) \prod_{i=1}^{n} \left( \sum_{j=0}^{r-1} x_{i,j} p^j \right)^{\mu_i} \\
&= \sum_{\boldsymbol{\mu} \in Supp(\bar{f})} \left( \sum_{s=0}^{r-1} a_{\boldsymbol{\mu},s} p^s \right) \prod_{i=1}^{n} \left( \sum_{k \in I(\mu_i, r)} c_{\mu_i, k} \left[ \prod_{j=0}^{r-1} x_{i,j}^{k_j} \right] p^{d(k)} \right) \\
&= \sum_{\boldsymbol{\mu} \in Supp(\bar{f})} \left( \sum_{s=0}^{r-1} a_{\boldsymbol{\mu},s} p^s \right) \left( \sum_{\substack{k^{(1)} \in I(\mu_1, r) \\ k^{(2)} \in I(\mu_2, r) \\ \cdots \\ k^{(n)} \in I(\mu_n, r)}} \prod_{i=1}^{n} c_{\mu_i, k^{(i)}} p^{d(k^{(i)})} \left[ \prod_{j=0}^{r-1} x_{i,j}^{k_j^{(i)}} \right] \right)
\end{aligned}$$

where the coefficients $c_{\mu_i,k}$ are the multinomial coefficients $\binom{\mu_i}{k_0, k_1, \cdots, k_{r-1}}$ and similarly for $c_{\mu_i, k^{(i)}}$.

Let us now introduce the following notations for convenience. Let $\mathbf{k} = (k^{(1)}, k^{(2)}, ..., k^{(n)})$ denote an element in the cartesian product, $\prod_{i=1}^{n} I(\mu_i, r)$. Let $I(\boldsymbol{\mu}, r)$ denote the set of all

such elements that satisfy the property that

$$d(k^{(1)}) + d(k^{(2)}) + \cdots + d(k^{(n)}) \leq r - 1. \tag{3.2.1}$$

Note that only the monomials that satisfy the above condition 3.2.1 matter in our $p$-adic estimation. It is convenient to denote $d(k^{(1)}) + d(k^{(2)}) + \cdots + d(k^{(n)})$ by $d(\mathbf{k})$.

**Example 3.2.1.**

Let $n = 2, r = 3$ and let $\boldsymbol{\mu} = (\mu_1, \mu_2)$ with $\mu_1, \mu_2 \geq 2$. Then recall that for $i = 1, 2$,

$$I(\mu_i, r) = \left\{ \begin{pmatrix} \mu_i \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_i - 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_i - 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \mu_i - 2 \\ 2 \\ 0 \end{pmatrix} \right\}.$$

Then

$$I(\boldsymbol{\mu}, r) = \left\{ \begin{pmatrix} \mu_1 \\ 0 \\ 0 \\ \mu_2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_1 \\ 0 \\ 0 \\ \mu_2 - 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_1 \\ 0 \\ 0 \\ \mu_2 - 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \mu_1 \\ 0 \\ 0 \\ \mu_2 - 2 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_1 - 1 \\ 1 \\ 0 \\ \mu_2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_1 - 1 \\ 1 \\ 0 \\ \mu_2 - 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_1 - 1 \\ 0 \\ 1 \\ \mu_2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \mu_1 - 2 \\ 2 \\ 0 \\ \mu_2 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

For $\mathbf{k} = \begin{pmatrix} k^{(1)} \\ k^{(2)} \end{pmatrix} = \begin{pmatrix} \mu_1 - 1 \\ 1 \\ 0 \\ \mu_2 - 1 \\ 1 \\ 0 \end{pmatrix}$, we have that

$$d(\mathbf{k}) = d(k^{(1)}) + d(k^{(2)}) = 1 + 1 = 2$$

for example.

Also, since these integer coefficients do not matter in our $p$-adic estimation, we may introduce $c_{\boldsymbol{\mu},\mathbf{k}}$ to denote the integer $\prod_{i=1}^{n} c_{\mu_i,k^{(i)}}$. With these abbreviations, we me rewrite the above expression for the $r$-**expansion** of $\bar{f}(\bar{\mathbf{x}})$ as

$$\bar{f}(\bar{\mathbf{x}}) = \sum_{\boldsymbol{\mu}\in Supp(\bar{f})} \left(\sum_{s=0}^{r-1} a_{\boldsymbol{\mu},s}p^s\right)\left(\sum_{\mathbf{k}\in I(\boldsymbol{\mu},r)} c_{\boldsymbol{\mu},\mathbf{k}}p^{d(\mathbf{k})}\prod_{i=1}^{n}\prod_{j=0}^{r-1}\left[x_{i,j}^{k_j^{(i)}}\right]\right)$$

or

$$\bar{f}(\bar{\mathbf{x}}) = \sum_{\boldsymbol{\mu}\in Supp(\bar{f})}\sum_{\mathbf{k}\in I(\boldsymbol{\mu},r)}\sum_{s=0}^{r-1} a_{\boldsymbol{\mu},s}c_{\boldsymbol{\mu},\mathbf{k}}\mathbf{x}^{\mathbf{k}}p^{d(\mathbf{k})+s} \tag{3.2.2}$$

where $\mathbf{x}^{\mathbf{k}}$ denotes the product, $\prod_{i=1}^{n}\prod_{j=0}^{r-1} x_{i,j}^{k_j^{(i)}}$.

Now, for $\bar{\mathbf{x}} = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) \in \left(\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}\right)^n$, if each of the $\bar{x}_i$ are represented by Teichmüller representatives $(x_{i,j})_{j=1,2,...,r-1}$, then on applying the character $\Theta^{(r)}\circ\tau(q,l,r)$ to the polynomial $\bar{f}(\bar{\mathbf{x}})$, we get

$$\begin{aligned}
\Theta^{(r)}\circ\tau(q,l,r)\left(\bar{f}(\bar{\mathbf{x}})\right) &= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})}\prod_{\mathbf{k}\in I(\boldsymbol{\mu},r)}\prod_{s=0}^{r-1}\left[\Theta^{(r)}\circ\tau(q,l,r)\left(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}}p^{d(\mathbf{k})+s}\right)\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})}\prod_{u=0}^{r-1}\prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ 0\le s\le r-1\\ d(\mathbf{k})+s=u}}\left[\Theta^{(r)}\circ\tau(q,l,r)\left(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}}p^{u}\right)\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})}\prod_{u=0}^{r-1}\prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ 0\le s\le r-1\\ d(\mathbf{k})+s=u}}\left[\prod_{j=0}^{al-1}\theta_{r-u}(a_{\boldsymbol{\mu},s}^{p^j}\mathbf{x}^{\mathbf{k}p^j})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})}\prod_{u=0}^{r-1}\prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ 0\le s\le r-1\\ d(\mathbf{k})+s=u}}\left[\prod_{i=0}^{l-1}\prod_{j=0}^{a-1}\theta_{r-u}(a_{\boldsymbol{\mu},s}^{p^j}\mathbf{x}^{\mathbf{k}p^{ia+j}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{i=0}^{l-1}\prod_{j=0}^{a-1}\prod_{\boldsymbol{\mu}\in Supp(\bar{f})}\prod_{u=0}^{r-1}\prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ 0\le s\le r-1\\ d(\mathbf{k})+s=u}}\left[\theta_{r-u}(a_{\boldsymbol{\mu},s}^{p^j}\mathbf{x}^{\mathbf{k}p^{ia+j}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \qquad (\#)
\end{aligned}$$

where the third equality follows from the basic theory we established in Chapter 2, and the fourth equality follows from the fact that $a_{\boldsymbol{\mu},s}^{q} = a_{\boldsymbol{\mu},s}$, and hence we have obtained

an analogue of Proposition 2.1.21 in the previous chapter.

Let us now follow a very similar analysis as we did in the single variable case.

**Definition 3.2.2.** For each $i \in \{0, 1, ..., l-1\}$ and for each $j \in \{0, 1, ..., a-1\}$, we define

$$F_{i,j}(\mathbf{x}) := \prod_{\boldsymbol{\mu} \in Supp(\bar{f})} \prod_{u=0}^{r-1} \prod_{\substack{\mathbf{k} \in I(\boldsymbol{\mu}, r) \\ 0 \leq s \leq r-1 \\ d(\mathbf{k})+s=u}} \left[\theta_{r-u}(a_{\boldsymbol{\mu},s}^{p^j} \mathbf{x}^{\mathbf{k}p^{ia+j}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \tag{3.2.3}$$

where $\mathbf{x} = (x_{i,j})_{\substack{i=1,2,...,n \\ j=0,1,...,r-1}}$, the $a_{\boldsymbol{\mu},s}$ are the Teichmüller digits of the coefficients $\bar{a}_{\boldsymbol{\mu}}$ as defined before and the $c_{\boldsymbol{\mu},\mathbf{k}}$ are the integer coefficients obtained from the multinomial expansions as discussed before and $\boldsymbol{\mu}$ runs over $Supp(\bar{f})$.

With the above definition we have

$$\Theta^{(r)} \circ \tau(q, l, r)\left(\bar{f}(\bar{\mathbf{x}})\right) = \prod_{i=0}^{l-1} \prod_{j=0}^{a-1} F_{i,j}(\mathbf{x}) \tag{3.2.4}$$

Let us now analyze the growth of the coefficients of the basic series $F_{0,0}(\mathbf{x})$. In order to emphasize the degree, $m$ of the polynomial, $\bar{f}$ (which is useful in determining the weight functions) we incorporate that into the notation. Consider

$$F_{0,0}^{(m)}(\mathbf{x}) := F_{0,0}(\mathbf{x}) = \prod_{\boldsymbol{\mu} \in Supp(\bar{f})} \prod_{u=0}^{r-1} \prod_{\substack{\mathbf{k} \in I(\boldsymbol{\mu}, r) \\ 0 \leq s \leq r-1 \\ d(\mathbf{k})+s=u}} \left[\theta_{r-u}(a_{\boldsymbol{\mu},s} \mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}.$$

For fixed $(u, \boldsymbol{\mu}, \mathbf{k}, s)$ with $\boxed{u = d(\mathbf{k}) + s}$, define $\boxed{F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) := \left[\theta_{r-u}(a_{\boldsymbol{\mu},s} \mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}}$, so that

$$F_{0,0}^{(m)}(\mathbf{x}) = \prod_{u=0}^{r-1} \prod_{\boldsymbol{\mu} \in Supp(\bar{f})} \prod_{\substack{\mathbf{k} \in I(\boldsymbol{\mu}, r) \\ 0 \leq s \leq r-1 \\ d(\mathbf{k})+s=u}} F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}).$$

Then we have the following proposition.

**Proposition 3.2.3.** *For fixed* $(u, \boldsymbol{\mu}, \mathbf{k}, s)$ *with* $\boxed{u = d(\mathbf{k}) + s}$,

$$F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) = \sum_{h^{(\mathbf{k})}=0}^{\infty} B_{(u,\boldsymbol{\mu},s)}(\mathbf{k}, h^{(\mathbf{k})}) \mathbf{x}^{\mathbf{k}h^{(\mathbf{k})}}$$

*where the coefficients* $B_{(u,\boldsymbol{\mu},s)}(\mathbf{k}, h^{(\mathbf{k})})$ *satisfy*

$$\operatorname{ord}_p B_{(u,\boldsymbol{\mu},s)}(\mathbf{k}, h^{(\mathbf{k})}) \geq \frac{h^{(\mathbf{k})}}{p^{r-1-d(\mathbf{k})-s}(p-1)} = \frac{h^{(\mathbf{k})}}{p^{r-1-u}(p-1)} \geq \frac{h^{(\mathbf{k})}}{p^{r-1-d(\mathbf{k})}(p-1)}.$$

*Proof.* We have that for some coefficients $b_h^{(r-u)}$ satisfying $\operatorname{ord}_p b_h^{(r-u)} \geq \frac{h}{p^{r-u-1}(p-1)}$,

$$\begin{aligned} F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(x) &= \left( \sum_{h=0}^{\infty} b_h^{(r-u)} \mathbf{x}^{\mathbf{k}h} \right)^{c_{\boldsymbol{\mu},\mathbf{k}}} \\ &= \prod_{j=0}^{c_{\boldsymbol{\mu},\mathbf{k}}} \sum_{h_j=0}^{\infty} b_{h_j}^{(r-d(\mathbf{k})-s)} \mathbf{x}^{\mathbf{k}h_j} \\ &= \sum_{h^{(\mathbf{k})}=0}^{\infty} B_{(u,\boldsymbol{\mu},s)}(\mathbf{k}, h^{(\mathbf{k})}) \mathbf{x}^{\mathbf{k}h^{(\mathbf{k})}} \end{aligned}$$

where

$$B_{(u,\boldsymbol{\mu},s)}(\mathbf{k}, h^{(\mathbf{k})}) = \sum \prod_{j=1}^{c_{\boldsymbol{\mu},\mathbf{k}}} b_{h_j}^{(r-d(\mathbf{k})-s)}$$

where the sum runs over $\mathbf{h} = (h_1, h_2, ..., h_{c_{\boldsymbol{\mu},\mathbf{k}}}) \in \mathbb{Z}_{\geq 0}^{c_{\boldsymbol{\mu},\mathbf{k}}}$ such that $\sum_{j=1}^{c_{\boldsymbol{\mu},\mathbf{k}}} h_j = h^{(\mathbf{k})}$. And we have

$$\begin{aligned} \operatorname{ord}_p B_{(u,\boldsymbol{\mu},s)}(\mathbf{k}, h^{(\mathbf{k})}) &\geq \inf \left\{ \sum_{j=1}^{c_{\boldsymbol{\mu},\mathbf{k}}} \operatorname{ord}_p b_{h_j}^{(r-d(\mathbf{k})-s)} : \sum_{j=1}^{c_{\boldsymbol{\mu},\mathbf{k}}} h_j = h^{(\mathbf{k})} \right\} \\ &\geq \sum_{j=1}^{c_{\boldsymbol{\mu},\mathbf{k}}} \frac{h_j}{p^{r-d(\mathbf{k})-s-1}(p-1)} \\ &= \frac{h^{(\mathbf{k})}}{p^{r-d(\mathbf{k})-s-1}(p-1)} \end{aligned}$$

by the $p$-adic analytic properties of the function $\theta_{r-d(\mathbf{k})-s}(t)$ established earlier. □

### 3.2.1 The Λ-diagram Weight Function

Let us now generalize the **level-$r$ Λ-diagram weight** in the multivariable case. As before, let us consider the definitions of a class of matrices that help us understand this weight function better.

**Definition 3.2.4.** For each $s = 0, 1, 2, ..., r-1$, $I(\boldsymbol{\mu}, r, s)$ be the subset of $I(\boldsymbol{\mu}, r)$ consisting of those $n$-tuples of monomial vectors $\mathbf{k}$ for which $d(\mathbf{k}) < r - s$. Let $\bar{\boldsymbol{\rho}}(\boldsymbol{\mu}, r, s)$ be the cardinality of $I(\boldsymbol{\mu}, r, s)$. The members of $I(\boldsymbol{\mu}, r, 0)$ are the same as the members of $I(\boldsymbol{\mu}, r)$ which are obtained by applying Lemma 3.1.1. For the multivariable case, we may arrange these members first by the order of the variable and then in a total order dictated by the lexicographic ordering of the corresponding partitions of integers as per Proposition 3.1.4. Then the sets $I(\boldsymbol{\mu}, r, 1), I(\boldsymbol{\mu}, r, 2), ...$ are simply truncations of the set $I(\boldsymbol{\mu}, r, 0)$. We may put them all together in a matrix $K(\boldsymbol{\mu}, r) := [I(\boldsymbol{\mu}, r, 0)\ \ I(\boldsymbol{\mu}, r, 1)\ \ ...\ \ I(\boldsymbol{\mu}, r, r-1)]$ that has $r$ rows and $\sum_{s=0}^{r-1} \bar{\boldsymbol{\rho}}(\boldsymbol{\mu}, r, s)$ columns.

**Example 3.2.5.** Let $r = 3$ and let $\boldsymbol{\mu} = (\mu_1, \mu_2)$ with $\mu_1 \geq 2$ and $\mu_2 \geq 2$. Then

$$K(\boldsymbol{\mu}, r) = \left[\begin{array}{cccccccc||ccc||c} \mu_1 & \mu_1 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1-1 & \mu_1-1 & \mu_1-2 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mu_2 & \mu_2-1 & \mu_2-1 & \mu_2-2 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Observe that the matrix is divided into three blocks of columns where the first block correspond to $s = 0$, the next block corresponds to $s = 1$ and the last block correspond to $s = 2$.

**Example 3.2.6.** Let $r = 3$ and let $\boldsymbol{\mu} = (\mu_1, \mu_2)$ with $\mu_1 = 2, \mu_2 = 1$. Then

$$K(\boldsymbol{\mu}, r) = \left[\begin{array}{cccccccc||ccc||c} \mu_1 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1-1 & \mu_1-1 & \mu_1-2 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mu_2 & \mu_2-1 & \mu_2-1 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

As with the single variable case, let us now modify the matrix $K(\boldsymbol{\mu}, r)$ slightly in order to accommodate the effect of $d(\mathbf{k})$ and $s$ for each column $\mathbf{k}$ in the matrix. We define the matrix $\underline{K}(\boldsymbol{\mu}, r)$ as follows.

**Definition 3.2.7.** Replace each column $\mathbf{k}$ in the matrix $K(\boldsymbol{\mu}, r)$ with the column $p^{r-1-d(\mathbf{k})-s}\mathbf{k}$. Recall that $d(\mathbf{k}) = \sum_{j=1}^{n} d(k^{(j)})$ and that $s$ corresponds to the block in which the column is in. We thus obtain the matrix $\underline{K}(\boldsymbol{\mu}, r)$. The columns of this matrix are denoted by $\underline{\mathbf{k}}$ so that $\underline{\mathbf{k}} = p^{r-1-d(\mathbf{k})-s}\mathbf{k}$ where $\mathbf{k}$ is the corresponding column in $K(\boldsymbol{\mu}, r)$.

**Example 3.2.8.** Let $r = 3$ and let $\boldsymbol{\mu} = (\mu_1, \mu_2)$ with $\mu_1 \geq 2$ and $\mu_2 \geq 2$. Then recall that

$$K(\boldsymbol{\mu}, r) = \left[\begin{array}{cccccccc||ccc||c} \mu_1 & \mu_1 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1-1 & \mu_1-1 & \mu_1-2 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mu_2 & \mu_2-1 & \mu_2-1 & \mu_2-2 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

and that the first block corresponds to $s = 0$, the next one corresponds to $s = 1$ and the last one corresponds to $s = 2$. Then, we have

$$\underline{K}(\boldsymbol{\mu}, r) = \left[\begin{array}{cccccccc||ccc||c} p^2\mu_1 & p\mu_1 & \mu_1 & \mu_1 & p(\mu_1-1) & \mu_1-1 & \mu_1-1 & \mu_1-2 & p\mu_1 & \mu_1 & \mu_1-1 & \mu_1 \\ 0 & 0 & 0 & 0 & p & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ p^2\mu_2 & p(\mu_2-1) & \mu_2-1 & \mu_2-2 & p\mu_2 & \mu_2-1 & \mu_2 & \mu_2 & p\mu_2 & \mu_2-1 & \mu_2 & \mu_2 \\ 0 & p & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

**Example 3.2.9.** Let $r = 3$ and let $\boldsymbol{\mu} = (\mu_1, \mu_2)$ with $\mu_1 = 2, \mu_2 = 1$. Recall that

$$K(\boldsymbol{\mu}, r) = \left[\begin{array}{ccccccc||ccc||c} \mu_1 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1-1 & \mu_1-1 & \mu_1-2 & \mu_1 & \mu_1 & \mu_1-1 & \mu_1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mu_2 & \mu_2-1 & \mu_2-1 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 & \mu_2 & \mu_2-1 & \mu_2 & \mu_2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Then, we have

$$\underline{K}(\boldsymbol{\mu}, r) = \left[\begin{array}{ccccccc||ccc||c} p^2\mu_1 & p\mu_1 & \mu_1 & p(\mu_1-1) & \mu_1-1 & \mu_1-1 & \mu_1-2 & p\mu_1 & \mu_1 & \mu_1-1 & \mu_1 \\ 0 & 0 & 0 & p & 1 & 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ p^2\mu_2 & p(\mu_2-1) & \mu_2-1 & p\mu_2 & \mu_2-1 & \mu_2 & \mu_2 & p\mu_2 & \mu_2-1 & \mu_2 & \mu_2 \\ 0 & p & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

**Definition 3.2.10.** The **level** $r$ **$\Lambda$-diagram** corresponding to the polynomial $\bar{f}$ is defined as the convex closure (hull) of the columns of the matrices $\underline{K}(\boldsymbol{\mu}, r)$ as $\boldsymbol{\mu}$ runs over $Supp(\bar{f})$ along with the origin when looking at them as vectors in $\mathbb{R}^{nr}$. We denote this by $\Lambda(\bar{f}, r)$, and we write $\Lambda(\bar{f}, r) = Conv\left(\{\underline{k} : \underline{k} \in \underline{K}(\boldsymbol{\mu}, r) : \boldsymbol{\mu} \in Supp(\bar{f})\} \cup \{\mathbf{0}\}\right)$.

**Definition 3.2.11.** Let $f = f(\mathbf{x})$ be the $r$-expansion of $\bar{f}(\bar{\mathbf{x}})$. Let $Cone_\Lambda(f)$ be the union in $\mathbb{R}^{nr}$ of all the rays from the origin passing through all the points in $\Lambda(\bar{f}, r)$. Let $M_\Lambda(f) := Cone_\Lambda(f) \cap \mathbb{Z}^{nr}$.

**Definition 3.2.12.** For convenience, as with the single variable case, it is useful to define the submatrices of $\underline{K}(\boldsymbol{\mu}, r)$ that consist only of the columns that correspond respectively to $s = 0$, $s = 1$, ..., $s = (r-1)$ and let us denote these by $\underline{K}_s(\boldsymbol{\mu}, r)$ for each $s = 0, 1, ..., (r-1)$.

The following proposition analogous to the corresponding proposition in the single variable case holds by the definition of the matrix $\underline{K}(\boldsymbol{\mu}, r)$.

**Proposition 3.2.13.** *From the above definitions, we have*

$$\Lambda(\bar{f}, r) = Conv\left(\{\underline{k} : \underline{k} \in \underline{K}_0(\boldsymbol{\mu}, r), \mu \in Supp(\bar{f})\} \cup \{\mathbf{0}\}\right)$$

*Proof.* The columns of $\underline{K}_s(\boldsymbol{\mu}, r)$ for $s \geq 1$ are simply convex combinations of a column of $\underline{K}_0(\boldsymbol{\mu}, r)$ along with the origin. □

By the above proposition, we observe that only the columns of $\underline{K}_0(\boldsymbol{\mu}, r)$ as $\mu$ runs over $Supp(\bar{f})$ matter for the $\Lambda$-diagram.

**Definition 3.2.14.** For $y = (y_1, y_2, ..., y_{r-1}) \in M_\Lambda(f)$, the **level** $r$ **$\Lambda$-diagram weight** (or simply the diagram weight when there is no confusion about which diagram), $w_\Lambda(y)$

is defined as the smallest nonnegative rational number $b$ such that $y \in b\Lambda(\bar{f}, r) := \{v \in \mathbb{R}^{nr} : bv \in \Lambda(\bar{f}, r)\}$.

**Proposition 3.2.15.** *The level $r$ $\Lambda$-diagram weight function $w_\Lambda$ satisfies the following properties:*

*For $\alpha, \beta \in M_\Lambda(f)$, we have*

*(i)* $w_\Lambda(\alpha) = 0 \iff \alpha = 0$.

*(ii)* $w_\Lambda(c\alpha) = cw_\Lambda(\alpha)$ *if* $c \geq 0$.

*(iii)* $w_\Lambda(\alpha + \beta) \leq w_\Lambda(\alpha) + w_\Lambda(\beta)$

*(iv) There exists a positive integer $D$ such that for all $\kappa \in M(f)$, $w_\Lambda(\kappa) \in \left(\frac{1}{D}\right)\mathbb{Z}$.*

*Proof.*
$(i), (ii)$ and $(iii)$ follows easily from the definition of the $\Lambda$-diagram as a convex closure. And $(iv)$ follows from an analogous argument as in Corollary 2.2.5. □

Now, analogous to the single variable case, from Proposition 3.2.3, we immediately deduce the following result.

**Proposition 3.2.16.** *For fixed $(u, \boldsymbol{\mu}, \mathbf{k}, s)$ with $u \in \{0, 1, ..., r-1\}$, $\boldsymbol{\mu} = (\mu_1, \mu_2, ..., \mu_n)$, $\mu_i \in \{1, 2, ..., m\}$ such that $|\boldsymbol{\mu}| \leq m$, $\mathbf{k} \in I(\boldsymbol{\mu}, r)$ and $u = d(\boldsymbol{k}) + s$, when the power series, $F_{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x})$ is written out as $\sum_v A_v \mathbf{x}^v$, then the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1}.$$

*Proof.* From Proposition 3.2.3, we have that

$$F_{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) = \sum_{h^{(\mathbf{k})}=0}^{\infty} B(\mathbf{k}, h^{(\mathbf{k})}) \mathbf{x}^{\mathbf{k}h^{(\mathbf{k})}}$$

where the coefficients $B(\mathbf{k}, h^{(\mathbf{k})})$ satisfy

$$\operatorname{ord}_p B(\mathbf{k}, h^{(\mathbf{k})}) \geq \frac{h^{(\mathbf{k})}}{p^{r-1-u}(p-1)}.$$

So, for $v = \mathbf{k}h^{(\mathbf{k})}$, we have

$$\begin{aligned} & \operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1} \\ \iff & \operatorname{ord}_p A_v \geq \frac{w_\Lambda(\mathbf{k}h^{(\mathbf{k})})}{p-1} \\ \iff & \operatorname{ord}_p A_v \geq \frac{h^{(\mathbf{k})} w_\Lambda(\mathbf{k})}{p-1} \end{aligned}$$

and

$$\operatorname{ord}_p A_v \geq \frac{h^{(\mathbf{k})}}{p^{r-1-u}(p-1)}.$$

Hence it suffices to prove that

$$\frac{1}{p^{r-1-u}} \geq w_\Lambda(\mathbf{k}) \iff w_\Lambda(p^{r-1-d(\mathbf{k})-s}\mathbf{k}) \leq 1.$$

But the last inequality is easily seen to be true by observing that $\underline{\mathbf{k}} := p^{r-1-d(\mathbf{k})-s}\mathbf{k}$ is simply a column in the matrix $\underline{K}(\boldsymbol{\mu}, r)$. □

We have the following lemma analogous to the single variable case.

**Lemma 3.2.17.** *Let $N$ be a positive integer, $K$ be a positive constant and for each $i = 1, 2, ..., N$, let $H_i(\mathbf{x}) = \sum_{j \in Supp(H_i)} C_{i,j}\mathbf{x}^j$ be a power series in several variables with the $j$ being nonnegative vectors and the coefficients belonging to $\mathbb{C}_p$ are such that for all $i, j$,*

$$\operatorname{ord}_p C_{i,j} \geq K w_\Lambda(j).$$

*Let $H(\mathbf{x}) = \prod_{i=1}^{N} H_i(\mathbf{x})$. Then when $H(\mathbf{x})$ is written out as $\sum_v A_v \mathbf{x}^v$, the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq K w_\Lambda(v)$$

*Proof.* Writing out the product, we have

$$\begin{aligned}\sum_v A_v \mathbf{x}^v = H(\mathbf{x}) &= \prod_{i=1}^N H_i(\mathbf{x}) \\ &= \prod_{i=1}^N \sum_j C_{i,j}\mathbf{x}^j \\ &= \sum_v \sum_{j_1+j_2+\ldots+j_N=v} \left(\prod_{i=1}^N C_{i,j_i}\right)\mathbf{x}^v\end{aligned}$$

Thus, the coefficients $A_v$ satisfy

$$\begin{aligned}\operatorname{ord}_p A_v &\geq \inf\left\{\sum_{i=1}^N \operatorname{ord}_p C_{i,j_i} : j_1+j_2+\ldots+j_N = v\right\} \\ &\geq \sum_{i=1}^N K w_\Lambda(j_i) \\ &\geq K w_\Lambda\left(\sum_{i=1}^N j_i\right) \\ &= K w_\Lambda(v).\end{aligned}$$

□

We finally arrive at

**Proposition 3.2.18.** *When the power series, $F_{(0,0)}^{(m)}(\mathbf{x})$ is written out as $\sum_v A_v \mathbf{x}^v$, the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1}$$

*Proof.* From the above proposition, we have that if $F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) = \sum_\ell C_\ell \mathbf{x}^\ell$, then the coefficients $C_\ell$ satisfy

$$\operatorname{ord}_p C_\ell \geq \frac{w_\Lambda(\ell)}{p-1}.$$

Then for

$$\sum_{v} A_v x^v = F_{0,0}^{(m)}(\mathbf{x}) = \prod_{u=0}^{r-1} \prod_{\boldsymbol{\mu} \in Supp(\bar{f})} \prod_{\substack{\mathbf{k} \in I(\boldsymbol{\mu}, r) \\ 0 \leq s \leq r-1 \\ d(\bar{\mathbf{k}})+s=u}} F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}),$$

the coefficients $A_v$ satisfy

$$\operatorname{ord}_p A_v \geq \frac{w_\Lambda(v)}{p-1}$$

by the preceding lemma. □

### 3.2.2 The Σ-diagram Weight Function

When we notice the definition of the Λ-diagram weight as in Definition 3.2.10 and the proof of Proposition 3.2.18 carefully, we observe that we can obtain *much better* estimates on the $p$-adic size of the coefficients of the power series $F_{(0,0)}^{(m)}(\mathbf{x})$ by taking into account the $p$-divisibility of the coefficients $\bar{a}_{\boldsymbol{\mu}}$ of the polynomial $\bar{f}(\bar{\mathbf{x}})$. We may thus improve our estimates by defining a *new* diagram weight function that takes this $p$-divisibility of the coefficients into account.

That is, for $\boldsymbol{\mu} \in Supp(\bar{f})$, recall that the $p$-adic expansion of the coefficient $\bar{a}_{\boldsymbol{\mu}}$ is given by

$$\bar{a}_{\boldsymbol{\mu}} = \sum_{s=0}^{r-1} a_{\boldsymbol{\mu},s} p^s$$

where the $a_{\boldsymbol{\mu},s}$ are the Teichmüller digits. Now if we define $\boxed{s^*(\boldsymbol{\mu}) := \min\{s : a_{\boldsymbol{\mu},s} \neq 0\}}$, then it is clear that it suffices to consider the columns of the matrix,

$$\underline{K}(\boldsymbol{\mu}, r) = \Big[ \underline{K}_0(\boldsymbol{\mu}, r) \;\Big|\; \underline{K}_1(\boldsymbol{\mu}, r) \;\Big|\; \ldots \;\Big|\; \underline{K}_{r-1}(\boldsymbol{\mu}, r) \Big]$$

that are columns of the blocks $\underline{K}_s(\boldsymbol{\mu}, r)$ for $s \geq s^*(\boldsymbol{\mu})$, in defining our diagram weight function. Also, since for all $s > s^*(\boldsymbol{\mu})$ each of the columns of $\underline{K}_s(\boldsymbol{\mu}, r)$ is a convex combination of a column of $\underline{K}_{s^*(\boldsymbol{\mu})}(\boldsymbol{\mu}, r)$ and the origin (analogous to Proposition 3.2.13), it suffices to consider only the matrix $\underline{K}_{s^*(\boldsymbol{\mu})}(\boldsymbol{\mu}, r)$ in the definition of our diagram weight.

We define the new diagram as follows.

**Definition 3.2.19.** The **level** $r$ **$\Sigma$-diagram** (or simply the **level** $r$ **diagram** when there is no possible confusion about which diagram) corresponding to the polynomial $\bar{f}$ is defined as the convex closure (hull) of the columns of the matrices $\underline{K}_{s^*(\boldsymbol{\mu})}(\boldsymbol{\mu}, r)$ as $\boldsymbol{\mu}$ runs over $Supp(\bar{f})$ along with the origin when looking at them as vectors in $\mathbb{R}^{nr}$. We denote this by $\Sigma(\bar{f}, r)$, and we write

$$\Sigma(\bar{f}, r) = Conv\left(\{\underline{k} : \underline{k} \in \underline{K}_{s^*(\boldsymbol{\mu})}(\boldsymbol{\mu}, r) : \boldsymbol{\mu} \in Supp(\bar{f})\} \cup \{\mathbf{0}\}\right).$$

**Definition 3.2.20.** Let $f = f(\mathbf{x})$ be the $r$-expansion of $\bar{f}(\bar{\mathbf{x}})$. Let $Cone_{\Sigma}(f)$ be the union in $\mathbb{R}^{nr}$ of all the rays from the origin passing through all the points in $\Sigma(\bar{f}, r)$. Let $M_{\Sigma}(f) := Cone(f) \cap \mathbb{Z}^{nr}$. Since the $\Sigma$-diagram is *better* than the $\Lambda$-diagram, we almost always use this preferred diagram for our estimates. We may thus abbreviate $Cone_{\Sigma}(f)$ and $M_{\Sigma}(f)$ as $Cone(f)$ and $M(f)$ respectively, for convenience.

Also, by the remark made earlier, we have the following obvious equality on the convex closures.

$$\begin{aligned} &Conv\left(\{\underline{k} : \underline{k} \in \underline{K}_s(\boldsymbol{\mu}, r) : s^*(\boldsymbol{\mu}) \leq s \leq (r-1), \boldsymbol{\mu} \in Supp(\bar{f})\} \cup \{\mathbf{0}\}\right) \\ &= Conv\left(\{\underline{k} : \underline{k} \in \underline{K}_{s^*(\boldsymbol{\mu})}(\boldsymbol{\mu}, r) : \boldsymbol{\mu} \in Supp(\bar{f})\} \cup \{\mathbf{0}\}\right) = \Sigma(\bar{f}, r) \end{aligned} \tag{3.2.5}$$

We now define the level $r$ $\Sigma$-diagram weight in an analogous manner.

**Definition 3.2.21.** For $y = (y_1, y_2, ..., y_{r-1}) \in M(f)$, the **level** $r$ **$\Sigma$-diagram weight** (or simply the diagram weight when there is no confusion about which diagram), $w_{\Sigma}(y)$ is defined as the smallest nonnegative rational number $b$ such that

$$y \in b\Sigma(\bar{f}, r) := \{v \in \mathbb{R}^{nr} : bv \in \Sigma(\bar{f}, r)\}.$$

**Proposition 3.2.22.** *The level $r$ $\Sigma$-diagram weight function $w_{\Sigma}$ satisfies the following properties:*

*For $\alpha, \beta \in M(f)$, we have*

*(i)* $w_\Sigma(\alpha) = 0 \iff \alpha = 0$.

*(ii)* $w_\Sigma(c\alpha) = cw_\Sigma(\alpha)$ *if* $c \geq 0$.

*(iii)* $w_\Sigma(\alpha + \beta) \leq w_\Sigma(\alpha) + w_\Sigma(\beta)$

*(iv) There exists a positive integer $D$ such that for all $\kappa \in M(f)$, $w_\Sigma(\kappa) \in \left(\frac{1}{D}\right)\mathbb{Z}$.*

*Proof.*
$(i), (ii)$ and $(iii)$ follows easily from the definition of the $\Sigma$-diagram as a convex closure. And $(iv)$ follows from an analogous argument as in Corollary 2.2.5. □

We may now strengthen Proposition 3.2.16 to the following proposition. Please pay attention to the small but significant change in the hypothesis of the following proposition when compared to that of Proposition 3.2.16.

**Proposition 3.2.23.** *For fixed $(u, \boldsymbol{\mu}, \mathbf{k}, s)$ with $s \geq s^*(\boldsymbol{\mu})$, $u \in \{0, 1, ..., r-1\}$, $\boldsymbol{\mu} = (\mu_1, \mu_2, ..., \mu_n) \in Supp(\bar{f})$, $\mu_i \in \{1, 2, ..., m\}$ such that $|\boldsymbol{\mu}| \leq m$, $\mathbf{k} \in I(\boldsymbol{\mu}, r)$ and $u = d(\boldsymbol{k}) + s$, when the power series, $F_{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x})$ is written out as $\sum_v A_v \mathbf{x}^v$, then the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq \frac{w_\Sigma(v)}{p-1}.$$

*Proof.* The proof is analogous to that of Proposition 3.2.16. But pay attention to the last part. From Proposition 3.2.3, we have that

$$F_{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) = \sum_{h^{(\mathbf{k})}=0}^{\infty} B(\mathbf{k}, h^{(\mathbf{k})}) \mathbf{x}^{\mathbf{k}h^{(\mathbf{k})}}$$

where the coefficients $B(\mathbf{k}, h^{(\mathbf{k})})$ satisfy

$$\operatorname{ord}_p B(\mathbf{k}, h^{(\mathbf{k})}) \geq \frac{h^{(\mathbf{k})}}{p^{r-1-u}(p-1)}.$$

So, for $v = \mathbf{k}h^{(\mathbf{k})}$, we have

$$\begin{aligned} & \operatorname{ord}_p A_v \geq \frac{w_\Sigma(v)}{p-1} \\ \iff & \operatorname{ord}_p A_v \geq \frac{w_\Sigma(\mathbf{k}h^{(\mathbf{k})})}{p-1} \\ \iff & \operatorname{ord}_p A_v \geq \frac{h^{(\mathbf{k})} w_\Sigma(\mathbf{k})}{p-1} \end{aligned}$$

and

$$\operatorname{ord}_p A_v \geq \frac{h^{(\mathbf{k})}}{p^{r-1-u}(p-1)}.$$

Hence it suffices to prove that

$$\frac{1}{p^{r-1-u}} \geq w_\Sigma(\mathbf{k}) \iff w_\Sigma(p^{r-1-d(\mathbf{k})-s}\mathbf{k}) \leq 1.$$

But the last inequality is easily seen to be true by observing that $\underline{\mathbf{k}} := p^{r-1-d(\mathbf{k})-s}\mathbf{k}$ is simply a column in the matrix $\underline{K}_s(\boldsymbol{\mu}, r)$ and $s \geq s^*(\boldsymbol{\mu})$ (cf. Equation 3.2.5). □

We have the following lemma analogous to Lemma 3.2.17.

**Lemma 3.2.24.** *Let $N$ be a positive integer, $K$ be a positive constant and for each $i = 1, 2, ..., N$, let $H_i(\mathbf{x}) = \sum_{j \in Supp(H_i)} C_{i,j}\mathbf{x}^j$ be a power series in several variables with the $j$ being nonnegative vectors and the coefficients belonging to $\mathbb{C}_p$ are such that for all $i, j$,*

$$\operatorname{ord}_p C_{i,j} \geq K w_\Sigma(j).$$

*Let $H(\mathbf{x}) = \prod_{i=1}^{N} H_i(\mathbf{x})$. Then when $H(\mathbf{x})$ is written out as $\sum_v A_v \mathbf{x}^v$, the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq K w_\Sigma(v)$$

*Proof.* Analogous to the proof of Lemma 3.2.17. □

We now deduce the stronger estimate based on the Σ-diagram weight.

**Proposition 3.2.25.** *When the power series, $F_{(0,0)}^{(m)}(\mathbf{x})$ is written out as $\sum_v A_v \mathbf{x}^v$, the coefficients $A_v$ satisfy*

$$\operatorname{ord}_p A_v \geq \frac{w_\Sigma(v)}{p-1}$$

*Proof.* From the above proposition, we have that if $F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) = \sum_\ell C_\ell \mathbf{x}^\ell$, then the coefficients $C_\ell$ satisfy

$$\operatorname{ord}_p C_\ell \geq \frac{w_\Sigma(\ell)}{p-1}.$$

Then for

$$\begin{aligned}\sum_v A_v x^v = F_{0,0}^{(m)}(\mathbf{x}) &= \prod_{u=0}^{r-1} \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ 0\leq s\leq r-1\\ d(\mathbf{k})+s=u}} F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) \\ &= \prod_{u=0}^{r-1} \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ s^*(\boldsymbol{\mu})\leq s\leq r-1\\ d(\mathbf{k})+s=u}} F_{0,0}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}),\end{aligned}$$

the coefficients $A_v$ satisfy

$$\operatorname{ord}_p A_v \geq \frac{w_\Sigma(v)}{p-1}$$

by Lemma 3.2.24. (Note that $F_{(0,0)}^{(u,\boldsymbol{\mu},\mathbf{k},s)}(\mathbf{x}) = 1$ if $s < s^*(\boldsymbol{\mu})$, and hence we have the second equality above). □

### 3.2.3 The Generalized Dwork Trace Formula

From Proposition 3.2.25 and the analogous Proposition 3.2.18, we can easily arrive at Dwork trace formulas with respect to the Σ-diagram and the Λ-diagram respectively.

**Remark 3.2.26.** As remarked before, since the Σ-diagram gives better estimates, we will always use the Σ-diagram throughout the rest of this thesis. However, the Λ-diagram does provide some useful insight, when we think of the worst case possibilities. For example, in the single variable case ($n = 1$), in the special case when $1, m \in Supp(\bar{f})$, $a_{1,0} \neq 0$ and $a_{m,0} \neq 0$, the Σ-diagram of $\bar{f}$ coincides with the Λ-diagram of $\bar{f}$. If,

moreover, $r = 2$ or $r = 3$, then the $\Lambda$-diagrams $\Lambda(\bar{f}, 2)$ and $\Lambda(\bar{f}, 3)$ as described in section 3.1.5 give us good intuitions about the general, worst case scenarios. We note carefully that the theory we develop in the rest of this thesis can be based either on the $\Sigma$-diagram or on the $\Lambda$ diagram. We will, from now on, stick to the $\Sigma$-diagram in developing our theory. With slight modifications (replacing $w_\Sigma$ with $w_\Lambda$, $M_\Sigma(f)$ with $M_\Lambda(f)$, etc.) we have an analogous theory in terms of the $\Lambda$-diagram.

We are now in a position to construct certain $p$-adic Banach spaces associated to the polynomial $\bar{f}$ as in the $r = 1$ case, that we discussed in Chapter 2. For each rational number $b \geq 0$, given a $p$-adic field, $K$, we may define the collection of formal power series,

$$B_{\bar{f}}(b, K) := \left\{ \sum_{\nu \in M(f)} A(\nu)\mathbf{x}^\nu : A(\nu) \in K, \inf_{\nu \in M(f)} \{\mathrm{ord}_p\, A(\nu) - w_\Sigma(\nu)b\} > -\infty \right\}.$$

As before, we will omit the field $K$ in the notation $B_{\bar{f}}(b, K)$ and simply write $B_{\bar{f}}(b)$ once we have chosen the field, $K$. The choice of the field depends on the denominator of $b$ and the positive integer, $D$ in Proposition 3.2.22. By Dwork's theory, we observe that the $B_{\bar{f}}(b)$ are $p$-adic Banach spaces and we have

**Proposition 3.2.27.** *For rational numbers $b' > b \geq 0$, we have that the inclusion map $\mathbf{i} : B_{\bar{f}}(b') \hookrightarrow B_{\bar{f}}(b)$ is completely continuous.*

And we observe that the space $B_{\bar{f}}(b)$ can be expressed in terms of smaller subspaces, $B_{\bar{f}}(b, c)$ for real numbers $c$ as follows. Define

$$B_{\bar{f}}(b, c) := \left\{ \sum_{\nu \in M(f)} A(\nu)\mathbf{x}^\nu : A(\nu) \in K, \mathrm{ord}_p\, A(\nu) \geq w_\Sigma(\nu)b + c \right\}$$

so that $B_{\bar{f}}(b) = \bigcup_{c \in \mathbb{R}} B_{\bar{f}}(b, c)$. Then the following lemma (analogous to Lemma 2.2.7) holds.

**Lemma 3.2.28.** *Let $b$ be a nonnegative rational number and let $c, c'$ be real numbers. Then the following assertions hold.*

1. $B_{\bar{f}}(b,c)B_{\bar{f}}(b,c') \subset B_{\bar{f}}(b,c+c')$

2. *If* $\xi(x) \in B_{\bar{f}}(b,c)$, *then* $\xi(x^p) \in B_{\bar{f}}(b/p,c)$

3. *If rational numbers* $b' > b > 0$, *then* $B_{\bar{f}}(b',c) \subset B_{\bar{f}}(b,c)$

**Corollary 3.2.29.** *The series* $F_{0,0}(\mathbf{x}) \in B_{\bar{f}}\left(\frac{1}{p-1},0\right) \subset B_{\bar{f}}\left(\frac{1}{p-1}\right)$.

*Proof.* It follows from Proposition 3.2.25. □

Now let $\sigma$ denote the *Frobenius* generator of $Gal(\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r}))$. Then for any Laurent series, $H(x) = \sum_{\nu} A(\nu)x^{\nu} \in \mathbb{Q}_q(\zeta_p)\left((x_1, x_2..., x_\ell)\right)$, we can define the element obtained by the action of $\sigma^i$ on its coefficients as $\boxed{H^{\sigma^i}(x) := \sum_{\nu} \sigma^i(A(\nu))x^{\nu}}$ for $i = 0, 1, 2, ..., (a-1)$. Then we have the following corollary.

**Corollary 3.2.30.**

*(a) For each* $i = 0, 1, ..., l-1$ *and* $j = 0, 1, ..., a-1$, *the series* $F_{i,j}(\mathbf{x}) = F_{0,0}^{\sigma^j}(\mathbf{x}^{p^{ia+j}}) \in B_{\bar{f}}\left(\frac{1}{p^{ia+j}(p-1)},0\right) \subset B_{\bar{f}}\left(\frac{1}{p^{ia+j}(p-1)}\right)$.

*(b) The series* $G(\mathbf{x}) := \prod_{i=0}^{l-1}\prod_{j=0}^{a-1} F_{i,j}(\mathbf{x}) \in B_{\bar{f}}\left(\frac{p}{q^l(p-1)},0\right) \subset B_{\bar{f}}\left(\frac{p}{q^l(p-1)}\right)$.

*Proof.* First we recall that

$$\begin{aligned}
F_{i,j}(\mathbf{x}) &= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{u=0}^{r-1} \prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r)\\ 0\le s\le r-1\\ d(\mathbf{k})+s=u}} \left[\theta_{r-u}(a_{\boldsymbol{\mu},s}^{p^j}\mathbf{x}^{\mathbf{k}p^{ia+j}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\theta_{r-d(\mathbf{k})-s}(a_{\boldsymbol{\mu},s}^{p^j}\mathbf{x}^{\mathbf{k}p^{ia+j}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\theta_{r-d(\mathbf{k})-s}\left(\sigma^j(a_{\boldsymbol{\mu},s})\mathbf{x}^{\mathbf{k}p^{ia+j}}\right)\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= F_{0,0}^{\sigma^j}(\mathbf{x}^{p^{ia+j}}).
\end{aligned}$$

Then it is clear from the above lemma and from the fact that $\operatorname{ord}_p \sigma^j(a_{\boldsymbol{\mu},s}) = \operatorname{ord}_p a_{\boldsymbol{\mu},s}$, that $F_{i,j}(\mathbf{x}) \in B_{\bar{f}}\left(\frac{1}{p^{ia+j}(p-1)}, 0\right) \subset B_{\bar{f}}\left(\frac{1}{p^{ia+j}(p-1)}\right)$. Part $(b)$ follows from part $(a)$ and applying the lemma again. $\square$

We now see that the Dwork trace formula extends naturally for the kind of exponential sums that we are looking at, for all $r \geq 1$.

# Chapter 4

# The Dwork Complex

In this chapter, we will construct the analogue of the *Dwork complex* corresponding to our exponential sums $S_l^*(q, r, \Theta^{(r)}, \bar{f})$ in the case $r > 1$ using the generalized Dwork trace formula that we derived in Chapter 3. The proofs are analogous to what we did at the end of Chapter 2 for the case when $r = 1$. We will begin with a summary of what we had in the previous chapter.

## 4.1 The Generalized Dwork Trace Formula

Let

$$\bar{f}(\bar{\mathbf{x}}) = \sum_{\mu \in Supp(\bar{f})} a_{\boldsymbol{\mu}} \bar{\mathbf{x}}^{\boldsymbol{\mu}}$$

be a polynomial in $(\mathbb{Z}_q/p^r\mathbb{Z}_q)[\bar{x}_1, \bar{x}_2, ..., \bar{x}_n]$ of degree $m$ as described in the previous chapter. Then

$$\begin{aligned}\Theta_r \circ \tau(q, l, r)\left(\bar{f}(\bar{\mathbf{x}})\right) &= \prod_{i=0}^{l-1}\prod_{j=0}^{a-1} F_{i,j}(\mathbf{x}) \\ &= \prod_{i=0}^{l-1}\prod_{j=0}^{a-1} F_{0,0}^{\sigma^j}(\mathbf{x}^{p^{ia+j}})\end{aligned}$$

where $\sigma$ is the Frobenius generator of $Gal\left(\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})\right)$, and the series $F_{i,j}(\mathbf{x})$ is in

the $p$-adic Banach space, $B_{\bar{f}}\left(\frac{1}{p^{ia+j}(p-1)}, 0\right) \subset B_{\bar{f}}\left(\frac{1}{p^{ia+j}(p-1)}\right)$.

Now, following the analogous arguments in Chapter 2 for the base case ($r = 1$), we can arrive at the generalized trace formula as follows.

Let $b$ be a nonnegative rational number. For $\xi(\mathbf{x}) = \sum_{\omega \in M(f)} C(\omega)\mathbf{x}^{\omega} \in B_{\bar{f}}(b, c)$, we define $\psi_q : B_{\bar{f}}(b, c) \to B_{\bar{f}}(qb, c)$ by $\psi_q(\xi(x)) := \sum_{\substack{\omega \in M(f) \\ q|\omega}} C(\omega)\mathbf{x}^{q^{-1}\omega} = \sum_{\nu \in M(f)} C(q\nu)\mathbf{x}^{\nu}$, where $\operatorname{ord}_p C(q\nu) \geq w_{\Sigma}(q\nu)b + c = w_{\Sigma}(\nu)qb + c$, and hence the map is well defined. Also, this map is a bounded (therefore, continuous) $K$-linear operator on $B_{\bar{f}}(b)$, since given a basis, $\{\pi_b^{w_{\Sigma}(\nu)}\mathbf{x}^{\nu} : \nu \in M(f)\}$ for $B_{\bar{f}}(b)$, we may take the set $\{\pi_b^{qw_{\Sigma}(\nu)}\mathbf{x}^{\nu} : \nu \in M(\bar{f})\}$ to be the basis for $B_{\bar{f}}(qb)$. We also observe that for $H \in B_{\bar{f}}(b)$, the operator, "multiplication by $H$", $H : B_{\bar{f}}(b) \to B_{\bar{f}}(b)$ defined by $H(F) := HF$ is a continuous $\mathbb{C}_p$-linear map. Then by Proposition 2.2.6, and by the fact that the composition of a continuous linear operator with a completely continuous linear operator is completely continuous [Ser62], we have that whenever $b > 0$, the composite, $i_q \circ \psi_q \circ H : B_{\bar{f}}(b) \to B_{\bar{f}}(b)$

$$B_{\bar{f}}(b) \xrightarrow{H} B_{\bar{f}}(b) \xrightarrow{\psi_q} B_{\bar{f}}(qb) \xrightarrow{i_q} B_{\bar{f}}(b)$$

is completely continuous, where $i_q$ is the inclusion map.

Now, let

$$G_r(\mathbf{x}) = \prod_{j=0}^{a-1} F_{0,j}(\mathbf{x}).$$

Then by [Ser62], the operator $\alpha : B_{\bar{f}}(b) \to B_{\bar{f}}(b)$ defined by $\boxed{\alpha := i_q \circ \psi_q \circ G_r}$, where $b = \dfrac{p}{q(p-1)}$ is completely continuous on the $p$-adic Banach space, $B_{\bar{f}}(b)$ over the discretely valued field $K$ of charecteristic zero. Hence,

$$\det(\mathbb{I} - t\alpha) = \exp\left(-\sum_{m=1}^{\infty} \frac{\operatorname{Tr}(\alpha^m)t^m}{m}\right) \tag{4.1.1}$$

where $\mathbb{I}$ is the identity endomorphism.

Then by Dwork's $p$-adic theory, we have the following analogous results. (Please refer to Chapter 2 for proofs).

**Proposition 4.1.1** (Analogue of Proposition 2.1.26 for $r > 1$)**.** *Let* $G(\mathbf{x}) = \prod_{i=0}^{l-1} G_r(\mathbf{x}^{q^i})$, *so that* $G(\mathbf{x}) = \prod_{i=0}^{l-1}\prod_{j=0}^{a-1} F_{i,j}(\mathbf{x})$. *If* $G(\mathbf{x})$ *is written out as*

$$G(\mathbf{x}) = \sum_{\nu} A(\nu)\mathbf{x}^{\nu},$$

*then*

$$S_l^*(q, r, \Theta^{(r)}, \bar{f}) = (q^l - 1)^{nr} \sum_{(q^l-1)|\nu} A(\nu).$$

*Proof.* We imitate the argument in the proof of proposition 2.1.26, noting that the character sum is over $x_{i,j}$ satisfying $x_{i,j}^{q^l-1} = 1$, for all $i = 1, 2, ..., n$, and $j = 0, 1, ..., r-1$. These $nr$ variables bring about the exponent $nr$ on the right hand side. □

**Proposition 4.1.2.** *Let* $b$ *be a positive rational number. If* $H(\mathbf{x}) = \sum_{\omega \in M(f)} A(\omega)\mathbf{x}^{\omega} \in B_{\bar{f}}(b)$, *then the trace,*

$$\mathrm{Tr}(i_q \circ \psi_q \circ H) = \sum_{\substack{\nu \in M(\bar{f}) \\ (q-1)|\nu}} A(\nu) = \sum_{\nu \in M(\bar{f})} A((q-1)\nu)$$

**Proposition 4.1.3.** *Let* $b$ *be a nonnegative rational number. If* $H(\mathbf{x}) \in B_{\bar{f}}(b)$, *then for any positive integer* $l$, *we have*

$$(i_q \circ \psi_q \circ H)^l = i_{q^l} \circ \psi_{q^l} \circ \prod_{j=0}^{l-1} H(\mathbf{x}^{q^j})$$

And finally we get the generalized trace formula,

**Theorem 4.1.4.** *(Dwork Trace Formula) For each positive integer,* $l$ *we have*

$$\boxed{S_l^*(q, r, \Theta^{(r)}, \bar{f}) = (q^l - 1)^{nr}\,\mathrm{Tr}(\alpha^l)}$$

*where* $\alpha = i_q \circ \psi_q \circ G_r$.

We will now obtain an analogous expression for the associated $L$-function in terms of Dwork's $\delta$-operator (with respect to $q$) defined as follows. For a rational function or Laurent series $P(t) \in K((t))$, we write $\boxed{P(t)^{\delta} := \frac{P(t)}{P(qt)}}$. Recall that the $\delta$-operator is multiplicative and an easy induction argument shows that on applying the $\delta$ operator $n$ times successively we get

$$P(t)^{\delta^n} = \prod_{j=0}^{n} P(q^j t)^{\binom{n}{j}(-1)^j} \tag{4.1.2}$$

$$= \left[\frac{P(t)}{P(qt)^{\binom{n}{1}}}\right] \left[\frac{P(q^2t)^{\binom{n}{2}}}{P(q^3t)^{\binom{n}{3}}}\right] ... P(q^n t)^{(-1)^n} \tag{4.1.3}$$

Then we have

**Theorem 4.1.5.** *Let* $N = nr$. *Then*

*(a)*

$$L^*(q, r, \Theta^{(r)}, \bar{f}, T) = \prod_{j=0}^{N} \left[\det(\mathbb{I} - q^j \alpha T)\right]^{(-1)^{(N-j+1)}\binom{N}{j}}$$

*(b)*

$$L^*(q, r, \Theta^{(r)}, \bar{f}, T)^{(-1)^{(N+1)}} = \det(\mathbb{I} - \alpha T)^{\delta^N}$$

*Proof.* From the trace formula (Theorem 4.1.4) we have

$$\begin{aligned} L^*(q, r, \Theta^{(r)}, \bar{f}, T) &= \exp\left(\sum_{l=1}^{\infty} S_l^*(q, r, \Theta^{(r)}, \bar{f}) \frac{T^l}{l}\right) \\ &= \exp\left(\sum_{l=1}^{\infty} (q^l - 1)^{nr} \operatorname{Tr}(\alpha^l) \frac{T^l}{l}\right) \\ &= \exp\left(\sum_{l=1}^{\infty} \sum_{j=0}^{nr} \binom{nr}{j} q^{lj} (-1)^{nr-j} \operatorname{Tr}(\alpha^l) \frac{T^l}{l}\right) \end{aligned}$$

$$
\begin{aligned}
&= \exp\left(\sum_{j=0}^{nr}\sum_{l=1}^{\infty}\binom{nr}{j}q^{lj}(-1)^{nr-j}\operatorname{Tr}(\alpha^l)\frac{T^l}{l}\right)\\
&= \prod_{j=0}^{nr}\exp\left(\sum_{l=1}^{\infty}\binom{nr}{j}q^{lj}(-1)^{nr-j}\operatorname{Tr}(\alpha^l)\frac{T^l}{l}\right)\\
&= \prod_{j=0}^{nr}\left[\exp\left(\sum_{l=1}^{\infty}\operatorname{Tr}(\alpha^l)\frac{(q^jT)^l}{l}\right)\right]^{\binom{nr}{j}(-1)^{nr-j}}\\
&= \prod_{j=0}^{nr}\left[\exp\left(-\sum_{l=1}^{\infty}\operatorname{Tr}(\alpha^l)\frac{(q^jT)^l}{l}\right)\right]^{\binom{nr}{j}(-1)^{nr-j+1}}\\
&= \prod_{j=0}^{nr}\left[\det\left(\mathbb{I}-q^j\alpha T\right)\right]^{\binom{nr}{j}(-1)^{nr-j+1}}
\end{aligned}
$$

where the last equality follows from Equation 4.1.1. Hence we have part (a). Finally, part (b) follows from Equation 4.1.2. □

As before, let us call the operator $\psi_q$ as the *Dwork operator* or the *Dwork inverse Frobenius operator* since it is essentially a "$q$-th root" map. We will also refer to the maps $q^j\alpha$ as the *Dwork Frobenius* (or just Frobenius) maps for simplicity when there is no possible confusion. As in Chapter 2, in the next section, we will realize these *Frobenius maps* as a chain map occurring on a certain complex.

## 4.2 Realizing the Frobenius as a Chain Map on a Complex

Throughout the rest of this discussion, we will assume that the field $K_q = \mathbb{Q}_q(\zeta_{p^r}, \tilde{\pi})$, where $\tilde{\pi}$ is a root of an Eisenstein polynomial $t^\lambda - (1-\zeta_{p^r}) \in \mathbb{Q}_p(\zeta_{p^r})[t]$ for a sufficiently large positive integer $\lambda$ such that $K_q$ is sufficiently ramified over $\mathbb{Q}_q$ so that $\zeta_{p^r} \in K_q$ and all our Banach spaces defined over $K = K_q$ have convenient choices for orthonormal bases. Also let $K_p = \mathbb{Q}_p(\zeta_{p^r}, \tilde{\pi})$. Then it is clear that $Gal(K_q/K_p)$ is isomorphic to $Gal(\mathbb{F}_q/\mathbb{F}_p)$ by an argument similar to that of Proposition 2.1.23. As before, we will first describe another useful map $\alpha_0 : B_{\bar{f}}\left(\frac{1}{p-1}\right) \to B_{\bar{f}}\left(\frac{1}{p-1}\right)$ which satisfies $\alpha_0^a = \alpha$. This decomposition helps us realize the Frobenius maps as a chain map due to the peculiar commutativity properties of $\alpha_0$. Let $\sigma \in Gal\left(K_q/K_p\right)$ be the Frobenius

generator. Then its inverse, $\sigma^{-1}$ induces a ring homomorphism $\sigma^{-1} : B_{\bar{f}}\left(\frac{p}{p-1}\right) \to B_{\bar{f}}\left(\frac{p}{p-1}\right)$ by acting on the coefficients of an element in $B_{\bar{f}}\left(\frac{p}{p-1}\right)$. We note that this induced map $\sigma^{-1}$ is *not* $K_q$-linear, although it is $K_p$-linear. We also define the $\psi_p$ linear operator very similar to the $\psi_q$ operator (that is, $\psi_p$ is the "$p$-th root" map). Then since $F_{0,0}(\mathbf{x}) \in B_{\bar{f}}\left(\frac{1}{p-1}, 0\right)$ we have the composite $\psi_p \circ F_{0,0}(\mathbf{x}) : B_{\bar{f}}\left(\frac{1}{p-1}\right) \to B_{\bar{f}}\left(\frac{p}{p-1}\right)$, where the *map* $F_{0,0}(x)$ refers to "multiplication by $F_{0,0}(x)$" as before. Then we define $\alpha_0$ to be the composite

$$B_{\bar{f}}\left(\frac{1}{p-1}\right) \xrightarrow{\psi_p \circ F_{0,0}} B_{\bar{f}}\left(\frac{p}{p-1}\right) \xrightarrow{\sigma^{-1}} B_{\bar{f}}\left(\frac{p}{p-1}\right) \xrightarrow{i_p} B_{\bar{f}}\left(\frac{1}{p-1}\right)$$

$\alpha_0 := i_p \circ \sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x})$, where $i_p$ is the inclusion. Since $\sigma^{-1}$ is *not* $K_q$-linear, so is $\alpha_0$ which is only a group homomorphism. However, $\alpha_0$ is $\sigma^{-1}$-*semilinear* over $K_q$ in the following sense: For $c \in K_q$ and $\xi \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$, we have that $c\xi \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$ and it is easy to see that $\alpha_0(c\xi) = \sigma^{-1}(c)\alpha_0(\xi)$. However,

$$\alpha_0^a(c\xi) = \sigma^{-a}(c)\alpha_0^a(\xi) = c\alpha_0^a(\xi).$$

Thus, the composite $\alpha_0^a$ is $K_q$-linear even though $\alpha_0$ is not. However $\alpha_0$ is $K_p$-linear since $\sigma$ fixes $K_p$.

**Remark 4.2.1.** Note that, in fact, the induced map $\sigma^{-1}$ and the maps $\psi_{p^j}$ (where $j$ is a positive integer) can be defined on all spaces $B_{\bar{f}}(b)$ when $b$ is a nonnegative rational number. And similarly, for any $H(\mathbf{x}) \in B_{\bar{f}}(b)$, the "multiplication by $H(\mathbf{x})$ map" is well defined for any nonnegative rational number, $b$. Also, for any other positive rational number $b' < b$, we have the following commutative diagrams

$$\begin{array}{ccc} B_{\bar{f}}(b) & \xrightarrow{\sigma^{-1}} & B_{\bar{f}}(b) \\ \downarrow i & & \downarrow i \\ B_{\bar{f}}(b') & \xrightarrow{\sigma^{-1}} & B_{\bar{f}}(b') \end{array} \qquad \begin{array}{ccc} B_{\bar{f}}(b) & \xrightarrow{H(\mathbf{x})} & B_{\bar{f}}(b) \\ \downarrow i & & \downarrow i \\ B_{\bar{f}}(b') & \xrightarrow{H(\mathbf{x})} & B_{\bar{f}}(b') \end{array} \qquad \begin{array}{ccc} B_{\bar{f}}(b) & \xrightarrow{\psi_{p^j}} & B_{\bar{f}}\left(p^j b\right) \\ \downarrow i & & \downarrow i \\ B_{\bar{f}}(b') & \xrightarrow{\psi_{p^j}} & B_{\bar{f}}\left(p^j b'\right) \end{array}$$

where $i$ denotes the inclusion maps. Hence, we may ignore specifying the exact domain of these maps which is usually inferred from the context when performing some compu-

tations. We also observe that $\psi_p^j = \psi_{p^j}$ for any positive integer $j$, analogous to what we had for $\psi_q$.

**Proposition 4.2.2.** *Let $H(\mathbf{x}) \in B_{\bar{f}}(b)$ for some $b \in \mathbb{Q}_{\geq 0}$ such that $b \leq \frac{1}{p-1}$. Then*

*(a)*

$$F_{0,0}(\mathbf{x}) \circ \sigma^{-1}\left(H(\mathbf{x})\right) = \sigma^{-1} \circ F_{0,0}^{\sigma}(\mathbf{x})\left(H(\mathbf{x})\right)$$

*(b)*

$$\psi_p \circ \sigma^{-1}\left(H(\mathbf{x})\right) = \sigma^{-1} \circ \psi_p\left(H(\mathbf{x})\right)$$

*(c) If $L(\mathbf{x}) \in B_{\bar{f}}\left(\dfrac{p}{q(p-1)}\right)$, then $\alpha_0^a(L(\mathbf{x})) = \alpha(L(\mathbf{x}))$.*

*Proof.* The proof is analogous to that of Proposition 2.2.17. For part $(c)$, we have

$$\begin{aligned}
\alpha_0^a(L(\mathbf{x})) &= (i_p \circ \sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x}))^a(L(\mathbf{x})) \\
&= (\sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x}))^a(L(\mathbf{x})) \\
&= (\sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x})) \circ (\sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x})) \circ ... \circ (\sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x}))(L(\mathbf{x})) \\
&= \left(\sigma^{-a} \circ (\psi_p \circ F_{0,0}^{\sigma^{a-1}}(\mathbf{x})) \circ (\psi_p \circ F_{0,0}^{\sigma^{a-2}}(\mathbf{x})) \circ ... \circ (\psi_p \circ F_{0,0}^{\sigma}(\mathbf{x})) \circ (\psi_p \circ F_{0,0}(\mathbf{x}))\right) \\
&\qquad\qquad (L(\mathbf{x})) \\
&= \left(\sigma^{-a} \circ \psi_p^a \circ F_{0,0}^{\sigma^{a-1}}(\mathbf{x}^{p^{a-1}}) F_{0,0}^{\sigma^{a-2}}(\mathbf{x}^{p^{a-2}}) ... F_{0,0}^{\sigma}(\mathbf{x}^p) F_{0,0}(\mathbf{x})\right)(L(\mathbf{x})) \\
&= \left(\psi_{p^a} \circ G_r(\mathbf{x})\right)(L(\mathbf{x})) \\
&= \left(i_q \circ \psi_q \circ G_r(\mathbf{x})\right)(L(\mathbf{x})) \\
&= \alpha(L(\mathbf{x}))
\end{aligned}$$

where the omissions of the inclusion maps $i_p$ and our slight abuses in notations make sense by Remark 4.2.1 above. □

Now, our goal is to construct a certain complex on which the Frobenius maps, $q^j\alpha$ act as a chain map. In order to construct such a complex, we need a good differential operator which acts as boundary maps on the complex. Recall that the emboldened variable $\mathbf{x}$ refers to $\prod_{i=1}^{n}\prod_{j=0}^{r-1} x_{i,j}$. As with the $r = 1$ case, it turns out that the operator

$x_{i,j}\frac{\partial}{\partial x_{i,j}}$ (defined in the usual way) has *good* commutativity properties with the maps $\psi_p$ and $\psi_q$ and hence we may construct a certain Koszul complex whose boundary maps are derived from these operators.

**Lemma 4.2.3.** *Let $b$ be a nonnegative rational number, $k$ a positive integer, $i \in \{1, 2, ..., n\}$ and $j \in \{0, 1, ..., r-1\}$. Then on $B_{\bar{f}}(b)$, we have*

*(a)*

$$p^k x_{i,j}\frac{\partial}{\partial x_{i,j}} \circ \psi_{p^k} = \psi_{p^k} \circ x_{i,j}\frac{\partial}{\partial x_{i,j}}$$

*(b)*

$$\sigma^{-1} \circ x_{i,j}\frac{\partial}{\partial x_{i,j}} = x_{i,j}\frac{\partial}{\partial x_{i,j}} \circ \sigma^{-1}$$

*Proof.* Analogous to the proof of Lemma 2.2.18. □

**Lemma 4.2.4.** *(Twist Lemma) Suppose that $F_{0,0}(\mathbf{x})$ can be written as $F_{0,0}(\mathbf{x}) = \dfrac{H(\mathbf{x})}{H^\sigma(\mathbf{x}^p)}$ for some invertible $H(\mathbf{x}) \in B_{\bar{f}}(b, 0)$ for some rational number $b$ such that $0 \leq b \leq \frac{1}{p-1}$. Then*

*(a)*

$$G_r(\mathbf{x}) = \frac{H(\mathbf{x})}{H(\mathbf{x}^q)}$$

*(b) On $B_{\bar{f}}(\frac{1}{p-1})$,*

$$\psi_p \circ F_{0,0}(\mathbf{x}) = \frac{1}{H^\sigma(\mathbf{x})} \circ \psi_p \circ H(\mathbf{x})$$

*And similarly, on $B_{\bar{f}}(\frac{p}{q(p-1)})$,*

$$\psi_q \circ G_r(\mathbf{x}) = \frac{1}{H(\mathbf{x})} \circ \psi_q \circ H(\mathbf{x})$$

*(Note that the multiplication by $H(\mathbf{x})$ acts on a much larger space, $B_{\bar{f}}(b)$ but the compositions are stable on the spaces indicated.)*

*(c) On $B_{\bar{f}}(\frac{1}{p-1})$,*

$$\sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x}) = \frac{1}{H(\mathbf{x})} \circ \sigma^{-1} \circ \psi_p \circ H(\mathbf{x})$$

*Proof.* The proof is analogous to that of Lemma 2.2.19 for the case when $r = 1$. □

The above commutativity properties motivate us to define the linear operators $L_{i,j} : B_{\bar{f}}\left(\frac{1}{p-1}\right) \to B_{\bar{f}}\left(\frac{1}{p-1}\right)$ given by

$$L_{i,j} := \frac{1}{H(\mathbf{x})} \circ x_{i,j} \frac{\partial}{\partial x_{i,j}} \circ H(\mathbf{x})$$

for $i = 1, 2, ..., n$, whenever we are able to write $F_{0,0}(\mathbf{x}) = \frac{H(\mathbf{x})}{H^{\sigma}(\mathbf{x}^p)}$. And in this case the operators $L_{i,j}$ enjoy very good commutativity properties and are useful in the construction of the complex. The following proposition shows that this is indeed the case.

**Proposition 4.2.5.** *Let $r \geq 2$. Then the splitting function, $\hat{\theta}_r(t) := \prod_{j=1}^{r} \theta_j(t)$ can be written as $\hat{\theta}_r(t) = \frac{\hat{\phi}_r(t)}{\hat{\phi}_r(t^p)}$ in terms of another convergent power series, $\hat{\phi}_r(t) \in \mathbb{Q}_q(\zeta_{p^r})[[t]]$ which converges for $\mathrm{ord}_p\, t > 1 + 1/p + ... + 1/p^{r-2} = \frac{p^r - p}{p^{r-1}(p-1)}$.*

*Proof.* For each $j \in \{1, 2, ..., r\}$, let us define $\boxed{\phi_j(t) := \prod_{i=0}^{\infty} \theta_j(t^{p^i})}$. Then this infinite product converges in the formal topology (topology of coefficientwise convergence) [Dwo62] of $\mathbb{C}_p[[t]]$ and we have

$$\begin{aligned}
\frac{\phi_j(t)}{\phi_j(t^p)} &= \frac{\prod_{i=0}^{\infty} \theta_j(t^{p^i})}{\prod_{i=1}^{\infty} \theta_j(t^{p^i})} \\
&= \prod_{i=0}^{\infty} \frac{\theta_j(t^{p^i})}{\theta_j(t^{p^{i+1}})} \\
&= \theta_j(t)
\end{aligned}$$

due to successive cancellations.

Let $\boxed{\hat{\phi}_r(t) := \prod_{j=1}^{r} \phi_j(t)}$ and thus we see that

$$\hat{\theta}_r(t) = \frac{\hat{\phi}_r(t)}{\hat{\phi}_r(t^p)}$$

that is,

$$\prod_{j=1}^{r} \theta_j(t) = \frac{\prod_{j=1}^{r} \phi_j(t)}{\prod_{j=1}^{r} \phi_j(t^p)}.$$

It remains to show the convergence of the $\phi_j(t)$ and $\hat{\phi}_r(t)$. Recall that $\theta_j(t) = \exp\left[\sum_{j=0}^{\infty} \frac{(\gamma_j t)^{p^j}}{p^j}\right]$ where $\gamma_j$ is a zero of $S(t) := \sum_{j=0}^{\infty} \frac{t^{p^j}}{p^j}$ such that $\operatorname{ord}_p \gamma_j = \frac{1}{p^{j-1}(p-1)}$. Then, we may write

$$\begin{aligned}
\phi_j(t) &= \prod_{i=0}^{\infty} \theta_j(t^{p^i}) \\
&= \prod_{i=0}^{\infty} \exp\left[\sum_{k=0}^{\infty} \frac{(\gamma_j t^{p^i})^{p^k}}{p^k}\right] \\
&= \exp\left[\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} \frac{(\gamma_j t^{p^i})^{p^k}}{p^k}\right] \\
&= \exp\left(\sum_{i=0}^{\infty} \beta_i^{(j)} t^{p^i}\right)
\end{aligned}$$

where the coefficients $\beta_i^{(j)}$ are given by $\beta_i^{(j)} = \sum_{k=0}^{i} \frac{\gamma_j^{p^k}}{p^k}$. Now, since $S(\gamma_j) = \sum_{j=0}^{\infty} \frac{\gamma_1^{p^j}}{p^j} = 0$, we have that $\beta_i^{(j)} = -\sum_{k=i+1}^{\infty} \frac{\gamma_j^{p^k}}{p^k}$ and therefore,

$$\begin{aligned}
\operatorname{ord}_p(\beta_i^{(j)}) &= \operatorname{ord}_p\left(-\sum_{k=i+1}^{\infty} \frac{\gamma_j^{p^k}}{p^k}\right) \\
&\geq \inf_{k \geq i+1} \operatorname{ord}_p\left(\frac{\gamma_j^{p^k}}{p^k}\right) \\
&= \inf_{k \geq i+1}\left[\frac{p^k}{p^{j-1}(p-1)} - k\right] \\
&= \frac{p^{i+1}}{p^{j-1}(p-1)} - (i+1) \qquad (4.2.1)
\end{aligned}$$

where the last equality holds for $i \geq 0$ due to the fact that the real valued function $g(y) = \frac{p^y}{p^{j-1}(p-1)} - y$ is increasing for $y \geq 1$. And therefore, $\frac{p^i}{p^{j-1}(p-1)} - i$ tends to $\infty$ as $i$ tends to $\infty$.

Now, when $\operatorname{ord}_p t > 1 + 1/p + 1/p^2 + ... + 1/p^{r-2} = \frac{p^r - p}{p^{r-1}(p-1)}$,

$$\begin{aligned}
\operatorname{ord}_p\left(\sum_{i=0}^{\infty} \beta_i^{(j)} t^{p^i}\right) &> \inf_{i\geq 0}\left(\operatorname{ord}_p(\beta_i^{(j)}) + p^i \frac{p^r - p}{p^{r-1}(p-1)}\right) \\
&\geq \frac{p}{p^{j-1}(p-1)} - 1 + \frac{p^r - p}{p^{r-1}(p-1)} \\
&\geq \frac{p}{p^{r-1}(p-1)} - 1 + \frac{p^r - p}{p^{r-1}(p-1)} \\
&= \frac{1}{p-1}.
\end{aligned}$$

Hence, $\phi_j(t) = \exp\left(\sum_{i=0}^{\infty} \beta_i^{(j)} t^{p^i}\right)$ converges for $\operatorname{ord}_p t > \frac{p^r - p}{p^{r-1}(p-1)}$ for all $j \in \{1, 2, ..., r\}$ and thus $\hat{\phi}_r(t)$ converges for $\operatorname{ord}_p t > \frac{p^r - p}{p^{r-1}(p-1)}$. □

**Corollary 4.2.6.** *There exists an invertible power series $H(\mathbf{x}) \in B_{\bar{f}}(0,0)$ such that $F_{0,0}(\mathbf{x}) = \dfrac{H(\mathbf{x})}{H^{\sigma}(\mathbf{x}^p)}$.*

*Proof.* Recall (please see the end of the previous chapter) that

$$\begin{aligned}
F_{0,0}(\mathbf{x}) &= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{u=0}^{r-1} \prod_{\substack{\mathbf{k}\in I(\boldsymbol{\mu},r) \\ 0\leq s\leq r-1 \\ d(\mathbf{k})+s=u}} [\theta_{r-u}(a_{\boldsymbol{\mu},s}\mathbf{x}^k)]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\theta_{r-d(\mathbf{k})-s}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}.
\end{aligned}$$

We may set $H(\mathbf{x}) = \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\phi_{r-d(\mathbf{k})-s}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}$, where the $\phi_j(t)$ are the series defined in the proof of the previous proposition. Then since $\sigma(a_{\boldsymbol{\mu},s}) = a_{\boldsymbol{\mu},s}^p$ and $\theta_j(t) = \phi_j(t)/\phi_j(t^p)$, we have that $F_{0,0}(\mathbf{x}) = \dfrac{H(\mathbf{x})}{H^{\sigma}(\mathbf{x}^p)}$. And it is easily seen that $H(\mathbf{x}) \in B_{\bar{f}}(0,0)$ (for instance, by an analogue of Lemma 2.2.7). □

Hence, indeed we can write $F_{0,0}(\mathbf{x}) = \dfrac{H(\mathbf{x})}{H^{\sigma}(\mathbf{x}^p)}$ and therefore we may define the linear operators

$$L_{i,j} = \frac{1}{H(\mathbf{x})} \circ x_{i,j} \frac{\partial}{\partial x_{i,j}} \circ H(\mathbf{x})$$

on the space $B_{\bar{f}}\left(\dfrac{1}{p-1}\right)$ for $i = 1, 2, ..., n$.

**Remark 4.2.7.** It is to be observed carefully, as in the base case when $r = 1$, that the operators $L_{i,j}$ are stable on the space $B_{\bar{f}}\left(\frac{1}{p-1}\right)$ even though the individual map "multiplication by $H(\mathbf{x})$" (defined on a bigger space, $B_{\bar{f}}(0)$) need not be stable on the subspace $B_{\bar{f}}\left(\frac{1}{p-1}\right)$. Let the $\phi_j(t)$ be the power series defined in Proposition 4.2.5. Writing $\phi_j(t) = \exp\beta^{(j)}(t)$ where $\beta^{(j)}(t) = \sum_{i=0}^{\infty} \beta_i^{(j)} t^{p^i}$ as in Proposition 4.2.5 with the coefficients $\beta_i^{(j)}$ satisfying

$$\operatorname{ord}_p \beta_i^{(j)} \geq \frac{p^{i+1}}{p^{j-1}(p-1)} - (i+1)$$

we observe that

$$\frac{1}{\exp\beta^{(j)}(t)} \circ t\frac{\partial}{\partial t} \circ \exp\beta^{(j)}(t) = t\frac{\partial}{\partial t} + t\frac{\partial\beta^{(j)}}{\partial t}$$

by the product rule and the chain rule of the derivative operator. In the same way, for $H(\mathbf{x}) = \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\phi_{r-d(\mathbf{k})-s}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}$, we have

$$\begin{aligned}
L_{i,j} &= \frac{1}{H(\mathbf{x})} \circ x_{i,j}\frac{\partial}{\partial x_{i,j}} \circ H(\mathbf{x}) \\
&= \frac{1}{\prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\phi_{r-d(\mathbf{k})-s}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}} \circ x_{i,j}\frac{\partial}{\partial x_{i,j}} \\
&\qquad \circ \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\phi_{r-d(\mathbf{k})-s}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \frac{1}{\prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\exp\beta^{(r-d(\mathbf{k})-s)}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}}} \circ x_{i,j}\frac{\partial}{\partial x_{i,j}} \\
&\qquad \circ \prod_{\boldsymbol{\mu}\in Supp(\bar{f})} \prod_{s=0}^{r-1} \prod_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} \left[\exp\beta^{(r-d(\mathbf{k})-s)}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right]^{c_{\boldsymbol{\mu},\mathbf{k}}} \\
&= \frac{1}{\exp\tilde{H}(\mathbf{x})} \circ x_{i,j}\frac{\partial}{\partial x_{i,j}} \circ \exp\tilde{H}(\mathbf{x}) \\
&= x_{i,j}\frac{\partial}{\partial x_{i,j}} + x_{i,j}\frac{\partial\tilde{H}}{\partial x_{i,j}}
\end{aligned}$$

where

$$\tilde{H}(\mathbf{x}) = \sum_{\boldsymbol{\mu}\in Supp(\bar{f})} \sum_{s=0}^{r-1} \sum_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} c_{\boldsymbol{\mu},\mathbf{k}}\beta^{(r-d(\mathbf{k})-s)}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}}).$$

Thus, in order to show that $L_{i,j}$ is stable on $B_{\bar{f}}\left(\frac{1}{p-1}\right)$, it suffices to show that the power series $x_{i,j}\frac{\partial \tilde{H}}{\partial x_{i,j}} \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$ since the operator $x_{i,j}\frac{\partial}{\partial x_{i,j}}$ is automatically stable on $B_{\bar{f}}\left(\frac{1}{p-1}\right)$ as the derivative only introduces integer coefficients. In fact, we can show something stronger as in the $r = 1$ case.

**Proposition 4.2.8.** *Let $\tilde{H}(\mathbf{x})$ be the be the power series as defined above. Then for each $i = 1, 2, ..., n$ and $j = 0, 1, ..., r-1$, we have*

$$x_{i,j}\frac{\partial \tilde{H}}{\partial x_{i,j}} \in B_{\bar{f}}\left(\frac{p}{p-1}, -1\right) \subset B_{\bar{f}}\left(\frac{1}{p-1}\right)$$

*Proof.* We have,

$$\begin{aligned} x_{i,j}\frac{\partial \tilde{H}}{\partial x_{i,j}} &= x_{i,j}\frac{\partial}{\partial x_{i,j}}\left(\sum_{\boldsymbol{\mu}\in Supp(\bar{f})}\sum_{s=0}^{r-1}\sum_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} c_{\boldsymbol{\mu},\mathbf{k}}\beta^{(r-d(\mathbf{k})-s)}(a_{\boldsymbol{\mu},s}\mathbf{x}^{\mathbf{k}})\right) \\ &= x_{i,j}\frac{\partial}{\partial x_{i,j}}\left(\sum_{\boldsymbol{\mu}\in Supp(\bar{f})}\sum_{s=s^*(\boldsymbol{\mu})}^{r-1}\sum_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} c_{\boldsymbol{\mu},\mathbf{k}}\sum_{\ell=0}^{\infty}\beta_\ell^{(r-d(\mathbf{k})-s)}a_{\boldsymbol{\mu},s}^{p^\ell}\mathbf{x}^{p^\ell\mathbf{k}}\right) \\ &= \sum_{\boldsymbol{\mu}\in Supp(\bar{f})}\sum_{s=s^*(\boldsymbol{\mu})}^{r-1}\sum_{\mathbf{k}\in I(\boldsymbol{\mu},r,s)} c_{\boldsymbol{\mu},\mathbf{k}}\sum_{\ell=0}^{\infty}\beta_\ell^{(r-d(\mathbf{k})-s)}a_{\boldsymbol{\mu},s}^{p^\ell}p^\ell k_j^{(i)}\mathbf{x}^{p^\ell\mathbf{k}}. \end{aligned}$$

Hence we may write $x_{i,j}\frac{\partial \tilde{H}}{\partial x_{i,j}} = \sum_{\nu\in M(f)} C(\nu)\mathbf{x}^\nu$ with coefficients, $C(\nu)$ given by

$$C(\nu) = \sum c_{\boldsymbol{\mu},\mathbf{k}}a_{\boldsymbol{\mu},s}^{p^\ell}k_j^{(i)}p^\ell\beta_\ell^{(r-d(\mathbf{k})-s)}$$

where the sum is over the set

$$S = \left\{(\boldsymbol{\mu},\ell,s,\mathbf{k}) \in Supp(f)\times\mathbb{Z}_{\geq 0}\times\{s^*(\boldsymbol{\mu}), s^*(\boldsymbol{\mu})+1, ..., r-1\}\times I(\boldsymbol{\mu},r,s) : p^\ell\mathbf{k} = \nu\right\}.$$

Then since $\operatorname{ord}_p c_{\boldsymbol{\mu},\mathbf{k}} \geq 0$, $\operatorname{ord}_p a_{\boldsymbol{\mu},s} \geq 0$ and $\operatorname{ord}_p k_j^{(i)} \geq 0$, by the inequality 4.2.1, we have that

$$\operatorname{ord}_p C(\nu) \geq \inf_{(\boldsymbol{\mu},\ell,s,\mathbf{k})\in S}(\operatorname{ord}_p\beta_\ell + \ell)$$

$$\geq \inf_{(\boldsymbol{\mu},\ell,s,\mathbf{k})\in S}\left(\frac{p^{\ell+1}}{p^{r-d(\mathbf{k})-s-1}(p-1)}-(\ell+1)+\ell\right)$$
$$= \inf_{(\boldsymbol{\mu},\ell,s,\mathbf{k})\in S}\left(\frac{p^{\ell+1}}{p^{r-d(\mathbf{k})-s-1}(p-1)}-1\right)$$
$$= \frac{p}{p-1}\left(\inf_{(\boldsymbol{\mu},\ell,s,\mathbf{k})\in S}\ \frac{p^{\ell}}{p^{r-d(\mathbf{k})-s-1}}\right)-1.$$

But since $w_\Sigma(p^{r-d(\mathbf{k})-s-1}\mathbf{k})\leq 1$ by the definition of the $\Sigma$-diagram weight, we have that

$$\frac{1}{p^{r-d(\mathbf{k})-s-1}}\geq w_\Sigma(\mathbf{k})$$

and hence,

$$\frac{p^{\ell}}{p^{r-d(\mathbf{k})-s-1}}\geq w_\Sigma(p^{\ell}\mathbf{k})=w_\Sigma(\nu).$$

Thus, we have that

$$\boxed{\operatorname{ord}_p C(\nu)\geq \frac{p}{p-1}w_\Sigma(\nu)-1}.$$

□

**Proposition 4.2.9.** *On* $B_{\bar{f}}\left(\frac{1}{p-1}\right)$, $pL_{i,j}\circ\alpha_0=\alpha_0\circ L_{i,j}$.

*Proof.*

$$\begin{aligned}
pL_i\circ\alpha_0 &= p\left[\frac{1}{H(\mathbf{x})}\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ H(\mathbf{x})\right]\circ\left[i_p\circ\sigma^{-1}\circ\psi_p\circ\frac{H(\mathbf{x})}{H^\sigma(\mathbf{x}^p)}\right]\\
&= p\left[\frac{1}{H(\mathbf{x})}\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ H(\mathbf{x})\right]\circ\left[i_p\circ\frac{1}{H(\mathbf{x})}\circ\sigma^{-1}\circ\psi_p\circ H(\mathbf{x})\right]\\
&= p\left[\frac{1}{H(\mathbf{x})}\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ i_p\circ\sigma^{-1}\circ\psi_p\circ H(\mathbf{x})\right]\\
&= p\left[\frac{1}{H(\mathbf{x})}\circ i_p\circ\sigma^{-1}\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ\psi_p\circ H(\mathbf{x})\right]\\
&= \left[\frac{1}{H(\mathbf{x})}\circ i_p\circ\sigma^{-1}\circ px_{i,j}\frac{\partial}{\partial x_{i,j}}\circ\psi_p\circ H(\mathbf{x})\right]\\
&= \left[\frac{1}{H(\mathbf{x})}\circ i_p\circ\sigma^{-1}\circ\psi_p\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ H(\mathbf{x})\right]\\
&= \left[\frac{1}{H(\mathbf{x})}\circ i_p\circ\sigma^{-1}\circ\psi_p\circ H(\mathbf{x})\circ\frac{1}{H(\mathbf{x})}\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ H(\mathbf{x})\right]\\
&= \left[i_p\circ\frac{1}{H(\mathbf{x})}\circ\sigma^{-1}\circ\psi_p\circ H(\mathbf{x})\right]\circ\left[\frac{1}{H(\mathbf{x})}\circ x_{i,j}\frac{\partial}{\partial x_{i,j}}\circ H(\mathbf{x})\right]
\end{aligned}$$

$$= \left[ i_p \circ \sigma^{-1} \circ \psi_p \circ \frac{H(\mathbf{x})}{H^\sigma(\mathbf{x}^p)} \right] \circ \left[ \frac{1}{H(\mathbf{x})} \circ x_{i,j} \frac{\partial}{\partial x_{i,j}} \circ H(\mathbf{x}) \right]$$
$$= \alpha_0 \circ L_{i,j}$$

where the chain of equalities follow from the commutativity properties proven above in this chapter: Proposition 4.2.2, Lemma 4.2.3 and Lemma 4.2.4. □

**Corollary 4.2.10.** *On* $B_{\bar{f}}\left(\frac{1}{p-1}\right)$, $qL_{i,j} \circ \alpha = \alpha \circ L_{i,j}$.

*Proof.* This result is a trivial consequence of Proposition 4.2.9 and statement $(c)$ in Proposition 4.2.2. □

We may now construct the Koszul complex on which the Frobenius maps $q^j\alpha$ act as a chain map. Let $M = B_{\bar{f}}\left(\frac{1}{p-1}\right)$. Then the linear operators $L_{i,j} : M \to M$ commute with eact other, that is, $L_{i,j}L_{u,v} = L_{u,v}L_{i,j}$ for all $i, u \in \{1, 2, ..., n\}$ and $j, v \in \{0, 1, ..., r-1\}$ since the mixed partial derivatives are equal independent of the order of differentiation. Let $S$ be the ring $\mathbb{Z}[L_{i,j} : i \in \{1, 2, ..., n\}, j \in \{0, 1, ..., r-1\}]$. Then $M$ has a natural $S$-module structure under the action $L_{i,j}.m = L_{i,j}(m)$ for $m \in M$.

Let $N = nr$. Let $\mathbf{L} = (L_{1,0}, L_{1,1}, ..., L_{n,r-1})$ which is rewritten as $\mathbf{L} = (\hat{L}_1, \hat{L}_2, ..., \hat{L}_N)$, where $L_{i,j} = \hat{L}_{(i-1)r+(j+1)}$, i.e., $\hat{L}_k = L_{i,j}$ with $i = \lfloor \frac{k-1}{r} \rfloor$ and $j$ is the integer in $\{0, 1, ..., r-1\}$ that equals $k-1$ modulo $r$. Now let $K^\bullet(\mathbf{L}, S)$ denote the Koszul cochain complex on $S$ with respect to $\mathbf{L}$. Let $K^\bullet(\mathbf{L}, M) := K^\bullet(\mathbf{L}, S) \otimes_S M$. We will construct this complex by first constructing $K^\bullet(\mathbf{L}, S)$ as follows. Set $K_S^i = 0$ for $i \in \mathbb{Z} - \{0, 1, 2, ..., N\}$. Then set $K_S^0 = S$ and $K_S^1 = S^N$. Set $K_S^i = \bigwedge^i(K_S^1)$, the $i$-th exterior power of the free $S$-module, $K_S^1$, of rank $N$, for $i = 2, 3, ..., N$. Let $\{e_1, e_2, ..., e_N\}$ be a basis for $K_S^1$. Then it is clear that $K_S^i$ is a free $S$-module of rank $\binom{N}{i}$ for $i = 2, 3, ..., N$ and they are given by

$$K_S^i = \bigoplus_{1 \le j_1 < j_2 < ... < j_i \le N} S(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

And the boundary maps $\partial_S^i : K_S^i \to K_S^{i+1}$ are given by

$$\partial_S^i(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) = \sum_{k=1}^{N} \hat{L}_k(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

for $i = 1, 2, ..., N-1$ and $\partial_S^0 : K_S^0 \to K_S^1$ is given by $\partial_S^0(1) = \sum_{k=1}^{N} \hat{L}_k e_k$.

Tensoring the complex $K^\bullet(\mathbf{L}, S)$ with $M$ over $S$, we get the complex $K^\bullet(\mathbf{L}, M)$ composed of free $S$-modules, $K^i$ given by $K^i = 0$ for $i \in \mathbb{Z} - \{0, 1, 2, ..., N\}$ and $K^1 = M$ and

$$K^i = \bigoplus_{1 \le j_1 < j_2 < ... < j_i \le N} M(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

for $i = 2, 3, ..., N$ with the boundary maps $\partial^i : K^i \to K^{i+1}$ given by

$$\partial^i(m e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) = \sum_{k=1}^{N} \hat{L}_k(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

for $i = 1, 2, ..., N-1$ and $\partial^0 : K^0 \to K^1$ is given by $\partial^0(m) = \sum_{k=1}^{N} \hat{L}_k(m) e_k$. It is easily seen that $\partial_S \partial_S = 0$ and $\partial\partial = 0$.

We may now define the $S$-linear map $\mathbf{Frob} : K^\bullet(\mathbf{L}, M) \to K^\bullet(\mathbf{L}, M)$ as follows. For $i = 1, 2, ..., N$, define $\mathbf{Frob}|^i : K^i \to K^i$ by

$$\mathbf{Frob}|^i = \bigoplus_{1 \le j_1 < j_2 < ... < j_i \le N} q^{N-i} \alpha(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})$$

and define $\mathbf{Frob}|^0 : K^0 \to K^0$ by $\mathbf{Frob}|^0 = q^N \alpha$.

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & K^0 \cong M & \xrightarrow{\partial^0} & K^1 \cong M^{\binom{N}{1}} & \xrightarrow{\partial^1} & K^2 \cong M^{\binom{N}{2}} & \xrightarrow{\partial^2} & ... & \xrightarrow{\partial^{N-1}} & K^N \cong M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle q^N \alpha} & & \downarrow{\scriptstyle \oplus_i q^{N-1}\alpha(e_i)} & & \downarrow{\scriptstyle \oplus_{i<j} q^{N-2}\alpha(e_i \wedge e_j)} & & & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & K^0 & \xrightarrow{\partial^0} & K^1 & \xrightarrow{\partial^1} & K^2 & \xrightarrow{\partial^2} & ... & \xrightarrow{\partial^{N-1}} & K^N & \longrightarrow & 0
\end{array}$$

Figure 4.1: Action of the Dwork Frobenius on the Dwork Complex: $r > 1$ case

**Proposition 4.2.11.** *The map* **Frob** *defined above is a chain map on the complex,* $K^\bullet(\mathbf{L}, M)$.

*Proof.* For each $i = 0, 1, 2, ..., N-1$ and $1 \leq j_1 < j_2 < ... < j_i \leq N$ and for $m \in M$, we have

$$\begin{aligned}
\partial^i \circ \mathbf{Frob}|^i \left[m(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})\right] &= \partial^i \left[q^{N-i}\alpha(m)(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})\right] \\
&= \sum_{k=1}^{N} \hat{L}_k \left(q^{N-i}\alpha(m)\right)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \sum_{k=1}^{N} q^{N-i-1}(q\hat{L}_k \circ \alpha)(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \sum_{k=1}^{N} q^{N-i-1}(\alpha \circ \hat{L}_k)(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \sum_{k=1}^{N} (q^{N-(i+1)}\alpha) \circ \hat{L}_k(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= q^{N-(i+1)}\alpha \circ \sum_{k=1}^{N} \hat{L}_k(m)(e_k \wedge e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i}) \\
&= \mathbf{Frob}|^{i+1} \circ \partial^i \left[m(e_{j_1} \wedge e_{j_2} \wedge ... \wedge e_{j_i})\right]
\end{aligned}$$

where the crucial fourth equality follows from Corollory 4.2.10. □

**Theorem 4.2.12.**

$$L^*(q, r, \Theta^{(r)}, \bar{f}, T)^{(-1)^{(N+1)}} = \prod_{j=0}^{N} \left[\det(\mathbb{I} - T\mathbf{Frob}|^{N-j})\right]^{(-1)^j}$$

*Proof.* The result follows from Theorem 4.1.5 and from the observation that

$$\left[\det(\mathbb{I} - q^j \alpha T)\right]^{\binom{N}{j}} = \det(\mathbb{I} - T\mathbf{Frob}|^{N-j})$$

for $j = 0, 1, ..., N$. □

The complex constructed above is the generalization of the *Dwork complex* for the $r > 1$ case and its cohomology is called the *Dwork cohomology*. And we also have an analogous statement on cohomology as we follow the discussion at the end of Chapter 2. That is, we have

**Theorem 4.2.13.**

$$\boxed{L^*(q,r,\Theta^{(r)},\bar{f},T)^{(-1)^{(N+1)}} = \prod_{j=0}^{N}\left[\det(\mathbb{I}-TH(\mathbf{Frob})|^{N-j}_{H^{N-j}(K^\bullet)})\right]^{(-1)^j}}.$$

# Chapter 5

# Rationality and Bombieri-Adolphson-Sperber Bounds on the Degree

In this chapter we will first prove the rationality of the $L$-function associated to the exponential sums we considered, using the classical methods of Dwork and Bombieri [Dwo60], [Bom66] generalized to our situation using our generalized trace formula and the Galois theory of Galois rings in the place of finite fields. We will then prove the Bombieri-Adolphson-Sperber bound [AS87a] on the degree of the $L$-function (or its reciprocal).

## 5.1 Rationality of the $L$-function

An immediate application of Dwork's trace formula is to prove the rationality of the associated $L$-function. One of the main ingredients in the proof of the rationality for the case when $r = 1$ is the fact that the function $\det(\mathbb{I} - \alpha T)$ is a *$p$-adically entire* function of $T$ as observed by Dwork ([Dwo60], [Ser62]), whence by Theorem 2.2.15, the associated $L$-function is $p$-adic meromorphic with infinite $p$-adic radius of meromorphy. A more comprehensive exposition of the proof of the rationality for the case when $r = 1$

can be found in [Kob84].

The argument for rationality ([Dwo60]) should easily extend to the case when $r > 1$ once we have the trace formula along with Galois theory for Galois rings. We have already seen that the functions $\theta_j(t)$ are $p$-adically *overconvergent* (that is, these functions converge on a disk of radius greater than 1 centered at the origin) (please recall Proposition 2.1.4 and Remark 2.2.9) for $j = 1, 2, ..., r$. Thus the *splitting function* [Bla03] $\hat{\theta}_r(t) := \prod_{j=1}^{r} \theta_j(t)$ is overconvergent. And this enabled us to construct a completely continuous endomorphism, $\alpha$ on a certain $p$-adic Banach space, namely, $B_{\bar{f}}(\frac{1}{p-1})$ and obtain a trace formula for the associated exponential sums, $S_l^*$, from which we can immediately express the associated $L$-function as a ratio of $p$-adically entire functions as in Theorem 4.1.5.

In this section let us describe the proof of the rationality in our case ($r > 1$) in more detail. We will follow the method of Bombieri [Bom66] to prove the rationality. Let us first state the key theorem (Dwork's Rationality Criterion).

**Theorem 5.1.1** (Dwork's Rationality Criterion: [Dwo60]: Theorem 3)**.** *If $L$ is an algebraic number field and $f(T) = \sum_{s=0}^{\infty} A_s T^s \in L[[T]]$, then $f$ is rational if and only if there exists a finite set, $S$, of primes of $L$ such that*

*(i) For each $\mathfrak{p} \notin S$, $|A_s|_{\mathfrak{p}} \leq 1$ for all integers $s \geq 0$.*

*(ii) For each $\mathfrak{p} \in S$, $f(T)$ is meromorphic in $\mathbb{C}_p$ in a circle $|T|_{\mathfrak{p}} \leq R_{\mathfrak{p}}$, where $\{R_{\mathfrak{p}}\}$ is the set of positive real numbers satisfying the condition*

$$\prod_{\mathfrak{p} \in S} R_{\mathfrak{p}} > 1.$$

In order to establish the rationality of our $L$-function,

$$L^*(q, r, \Theta^{(r)}, \bar{f}, T) = L^*(\bar{f}, T)$$

we make the following observations.

**Lemma 5.1.2.**

$$L^*(\bar{f}, T) \in \mathbb{Q}(\zeta_{p^r})[[T]]$$

*Proof.* This trivially follows from the fact that the sums $S_l^* = S_l^*(q, r, \Theta^{(r)}, \bar{f}) \in \mathbb{Q}(\zeta_{p^r})$ for all integers $l \geq 1$. □

**Lemma 5.1.3.** *$L^*(\bar{f}, T)$ is p-adically meromorphic with infinite radius of meromorphy on $\mathbb{C}_p$.*

*Proof.* By Theorem 4.1.5, $L^*(\bar{f}, T)$ is a ratio of finite products of Fredholm determinants, all of which are $p$-adically entire since the *Dwork Frobenius operator*, $\alpha$ and its $q^j$-multiples are completely continuous [Ser62] on the $p$-adic Banach space, $B_{\bar{f}}(\frac{1}{p-1})$. □

**Lemma 5.1.4.** *$L^*(\bar{f}, T)$ has a nonzero Archimedean radius of convergence, and hence a nonzero radius of meromorphy, $R_\infty^{(m)}$ associated to the prime $\infty$.*

*Proof.* Observe that the Archimedean absolute values of our exponential sums $S_l^* = S_l^*(q, r, \Theta^{(r)}, \bar{f})$ are bounded as follows:

$$|S_l^*(q, r, \Theta^{(r)}, \bar{f})| \leq \sum_{\bar{x} \in (\mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l})^n} \left|\Theta^{(r)} \circ \tau(q, l, r)(\bar{f}(\bar{x}))\right| = q^{lnr}$$

and thus the series $L^*(\bar{f}, T)$ is majorized by the power series, $\exp\left(\sum_{l=1}^{\infty} \frac{q^{lnr}T^l}{l}\right) = \frac{1}{1 - q^{nr}T}$, and the geometric series converges for $|T| < q^{-nr}$. □

Let us now state the other important lemma that generalizes Bombieri's lemma ([Bom66]: Lemma 1) to our situation, and that finally establishes the rationality of our $L$-function.

**Lemma 5.1.5.** *The coefficients $A_s$ of the Taylor series (about the origin) for $L^*(\bar{f}, T)$ are algebraic integers in the number field generated by a primitive $p^r$-th root of unity.*

We shall, in fact, prove the following (with more generality).

**Lemma 5.1.6.** *Let $R$ be the Galois ring $\mathbb{Z}_q/p^r\mathbb{Z}_q$. Let $A_1, A_2, ..., A_n$ be arbitrary subsets of $J_r := \{0, 1, 2, ..., r-1\}$. Let $A$ denote the $n$-uple, $(A_1, A_2, ..., A_n)$. For each integer $l$, let $R_l$ denote the degree-$l$ Galois ring extension of $R$, and let $S_l^{A,r}(\bar{f})$ denote the exponential sum as defined in Chapter 1, for the multivariable case, that is,*

$$S_l^{A,r}(\bar{f}) = S_l^{A,r}(q, r, \Theta^{(r)}, \bar{f}) := \sum_{x \in \mathcal{T}_l^{A,r}} \Theta^{(r)} \circ \tau(q, l, r)(\bar{f}(x))$$

*where*

$$\mathcal{T}_l^{A,r} = \mathcal{T}_l^{(A_1,...,A_n),r}$$
$$:= \left\{ x = (x_1, x_2, ..., x_n) = \left( \sum_{j=0}^{r-1} x_{1,j}p^j, \ldots, \sum_{j=0}^{r-1} x_{n,j}p^j \right) \in R_l^n : \begin{cases} x_{i,j} \neq 0, & \text{if } j \in A_i \\ x_{i,j} = 0, & \text{if } j \notin A_i \end{cases} \right\} \quad (5.1.1)$$

*where $\sum_{j_i=0}^{r-1} x_{i,j}p^j$ is the $p$-adic representation of the variable $x_i$ in the ring $R_l$ and the digits $x_{i,j}$ take Teichmüller representatives. Let $L^{A,r}(\bar{f}, T)$ denote the associated $L$-function, that is,*

$$L^{A,r}(\bar{f}, T) = \exp\left( \sum_{l=1}^{\infty} \frac{S_l^{A,r}(\bar{f})T^l}{l} \right).$$

*Then the coefficients $A_s$ of the Taylor series (about the origin) for $L^{A,r}(\bar{f}, T)$ are algebraic integers in the number field generated by a primitive $p^r$-th root of unity.*

Before proving these lemmas, let us first review the theory of 0-cycles for varieties over perfect fields (please see [Mon70]) and generalize this theory for affine varieties over Galois rings.

### 5.1.1 Theory of 0-Cycles for Affine Varieties over Galois Rings

We will follow the approach given in Monsky's account [Mon70] and generalize the theory of 0-cycles for affine varieties over Galois rings. We will also refer to [Wan03] for the basic results about Galois theory for Galois rings.

Let $R$ denote the Galois ring, $\mathbb{Z}_q/p^r\mathbb{Z}_q$. For each integer $l$, let $R_l$ denote the degree-$l$ Galois ring extension of $R$. Let $\bar{R}$ denote the ring $\mathbb{Z}_q^{(u)}/p^r\mathbb{Z}_q^{(u)}$ where $\mathbb{Z}_q^{(u)}$ is the ring of

integers of the maximal unramified extension, $\mathbb{Q}_q^{(u)}$ of $\mathbb{Q}_q$ in its algebraic closure, $\bar{\mathbb{Q}}_q$. The ring $\bar{R}$ is also denoted by $GR(p^r, \infty)$ and it is analogous to the algebraic closure of a finite field in a sense (please see [McD74]: Exercise XVI.6). For each pair of positive integers $d, e$ with $d|e$, let $Gal(R_e/R_d)$ (and recall that $R_1 = R$) denote the Galois group of $R_e$ over $R_d$ (that is, the group of automorphisms of $R_e$ fixing $R_d$ [Wan03]). We define the *absolute Galois group* of $\bar{R}$ over $R$ (denoted by $Gal(\bar{R}/R)$) to be the group of automorphisms of $\bar{R}$ that fix $R$. It can be shown that

$$Gal(\bar{R}/R) \cong Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong Gal(\mathbb{Q}_q^{(u)}/\mathbb{Q}_q)$$

where $\bar{\mathbb{F}}_q$ is the algebraic closure of the finite field $\mathbb{F}_q$ with $q$ elements, as follows.

We note (please see [Wan03]: Theorem 14.30) for integers $d, e$ with $d|e$, the group of automorphisms of the ring $R_e$ fixing every element of the ring $R_d$, $Gal(R_e/R_d)$ is generated by the *generalized Frobenius* generator. If $R_e = R_d[\xi]$, where $\xi$ is an element of order $q^e - 1$ in $R_e$ and is a root of a monic basic primitive polynomial $h(x)$ of degree $e/d$ over $R_d$ and dividing $x^{q-1} - 1$ in $R_d[x]$, the *generalized Frobenius* generator, $\sigma$ is defined by

$$\sigma\left(a_0 + a_1\xi + ... + a_{e/d-1}\xi^{e/d-1}\right) = a_0 + a_1\xi^q + ... + a_{e/d-1}\xi^{(e/d-1)q}$$

for all $a_0, a_1, ..., a_{e/d-1} \in R_d$, and that it acts on the Teichmüller digits of the $p$-adic representation of an element as the $q^d$-power map, that is, if $a = a_0 + a_1 p + ... + a_{r-1}p^{r-1}$ is an element of $R_d$ with its $p$-adic representation, then

$$\sigma(a) = \sigma(a_0 + a_1 p + ... + a_{r-1}p^{r-1}) = a_0^{q^d} + a_1^{q^d} p + ... + a_{r-1}^{q^d} p^{r-1}.$$

Now, since $\mathbb{Q}_q^{(u)} = \bigcup_{f=1}^{\infty} \mathbb{Q}_{q^f}$, and since $Gal(\mathbb{Q}_{q^f}/\mathbb{Q}_q) \cong Gal(\mathbb{F}_{q^f}/\mathbb{F}_q)$ (as we proved in Chapter 2), the inverse limit,

$$\varprojlim Gal(\mathbb{Q}_{q^f}/\mathbb{Q}_q) \cong \varprojlim Gal(\mathbb{F}_{q^f}/\mathbb{F}_q) \cong Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) \tag{5.1.2}$$

is isomorphic to $Gal(\mathbb{Q}_q^{(u)}/\mathbb{Q}_q)$.

On the other hand, by the isomorphisms of Galois groups of Galois ring extensions with those of the corresponding finite field extensions ([Wan03]: Theorem 14.32, Corollary 14.33), we also have an isomorphism on the inverse limits,

$$\varprojlim Gal(R_f/R) \cong \varprojlim Gal(\mathbb{F}_{q^f}/\mathbb{F}_q)$$

and thus,

$$Gal(\bar{R}/R) \cong Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q).$$

Hence, it follows that

$$Gal(\bar{R}/R) \cong Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong Gal(\mathbb{Q}_q^{(u)}/\mathbb{Q}_q).$$

Now, let $V$ be an affine variety defined over the ring $R$, (defined by a set of polynomial equations with coefficients in $R$; we do not require that the ideal generated by the associated polynomials is prime). We define the *zeta function* of $V$ to be the formal power series,

$$\boxed{Z(V,T) := \exp\left(\sum_{l=1}^{\infty} \frac{N_l(V)T^l}{l}\right)}$$

where $N_l(V)$ is the number of $R_l$-rational points of $V$. We may thus identify $V$ with its set of $\bar{R}$-rational points. We now define a 0-*cycle* $D$ on $V$ to be a formal $\mathbb{Z}$-linear combination of points of $V$. We say that $D$ is $R$-*rational* if it is invariant under the action of the Galois group $Gal(\bar{R}/R)$. If $P$ is a point of $V$ and $\{P_i\}$ is its orbit of $P$ under $Gal(\bar{R}/R)$, then $\sum_i P_i$ is called a *prime* $R$-*rational* 0-*cycle*. The *degree* of a 0-cycle, $D = \sum_i n_i P_i$ is defined to be the sum $\sum_i n_i$. And we say that a 0-cycle is $D = \sum_i n_i P_i$ is called *positive* if all the $n_i$ are nonnegative.

**Proposition 5.1.7.** *The* $R$*-rational* 0*-cycles form a free abelian group on the prime* $R$*-rational* 0*-cycles.*

*Proof.* It is clear that any finite collection of distinct prime $R$-rational 0-cycles are $\mathbb{Z}$-linearly independent (the 0-cycles are a free abelian group over the $\bar{R}$-rational points

of $V$) and that the free abelian group generated by the prime $R$-rational 0-cycles is a subgroup of the group of all $R$-rational 0-cycles on $V$. Now we claim that the prime $R$-rational 0-cycles generate the group of all $R$-rational 0-cycles. To see this we observe that any $R$-rational 0-cycle, $D = \sum_{i=1}^{k} n_i P_i$ with the $P_i$ distinct and the $n_i \neq 0$ is generated by prime $R$-rational 0-cycles. We can prove this by strong induction on $k$. Given such a 0-cycle $D$, we define its support, $Supp(D) := \{P_1, P_2, ..., P_k\}$. When $k = 1$, since $D$ is invariant under $Gal(\bar{R}/R)$, it follows that $P_1$ is a prime $R$-rational 0-cycle. Now assume that any such $R$-rational 0-cycle is generated by prime $R$-rational 0-cycles whenever $k \leq m$. Now consider an $R$-rational 0-cycle, $D = \sum_{i=1}^{m+1} n_i P_i$ with the $n_i \neq 0$ and the $P_i$ distinct. Let $\{Q_i : i = 1, 2, ..., d\}$ be the orbit of $P_1$ (with $Q_1 = P_1$) under the action $Gal(\bar{R}/R)$ and hence $\sum_{i=1}^{d} Q_i$ is the prime 0-cycle associated to $P_i$. It is clear that $1 \leq d \leq (m+1)$, and that the $Q_i$ are in $Supp(D)$. Suppose that $Q_i = P_{j_i}$ for some indices $j_i \in \{2, 3, ..., m+1\}$ for $i = 2, 3, ..., d$. Then it is clear that $n_{j_i} = n_1$ for all $i = 2, 3, ..., d$. If $d < (m+1)$, then $D - n_1 \sum_{i=1}^{d} Q_i$ is an $R$-rational 0-cycle which is generated by the prime ones by induction hypothesis and hence the result follows. If $d = m + 1$, then $D$ is generated by the prime $R$-rational 0-cycle, $\sum_{i=1}^{d} Q_i$, and hence we are done. □

We will now generalize Monsky's theorem ([Mon70]: Theorem 2.1) to our setting.

**Theorem 5.1.8.** *For each integer $s$, let $A_s$ be the number of positive $R$-rational 0-cycles of degree $s$ on $V$, let $M_s$ be the number of prime $R$-rational 0-cycles of degree $s$ on $V$ and let $N_s$ be the number of $R_s$-rational points of $V$. Then the following three formal power series are equal.*

*(a)* $\sum_{s=0}^{\infty} A_s T^s$

*(b)* $\prod_{s=1}^{\infty} (1 - T^s)^{-M_s}$

*(c)* $\exp\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right)$

*Proof.* Monsky's proof applies. However, we use the analogous Galois theory for Galois rings.

The power series $(b)$ can be written as

$$\begin{aligned}\prod_{d=1}^{\infty}(1-T^d)^{-M_d} &= \prod_{d=1}^{\infty}\sum_{l=1}^{\infty}(-1)^l\binom{-M_d}{l}T^{ld} \\ &= \sum_{l=1}^{\infty}\prod_{d=1}^{\infty}(-1)^l\binom{-M_d}{l}T^{ld}\end{aligned}$$

Calling the coefficients $(-1)^l\binom{-M_d}{l}$ as $N_d^{ld}$, we note that this number counts the number of distinct ways we get positive 0-cycles of degree $ld$ from $M_d$ prime 0-cycles of degree $d$. We then see that the coefficient of $T^s$ in the series $(b)$ is given by

$$\sum_{\substack{r_1,r_2,\ldots,r_k\in\mathbb{Z}_{\geq 0}\\ d_1<d_2<\ldots<d_k\in\mathbb{Z}_{\geq 0}\\ k\in\mathbb{Z}_{\geq 0}:\sum_{i=1}^{k}r_id_i=s}}\prod_{i=1}^{k}N_{d_i}^{r_id_i}$$

and by the previous proposition, this is precisely $A_s$. (Note that $A_0 = 1$).

By Galois theory of Galois rings, we find that

$$N_s = \sum_{d|s} dM_d. \tag{5.1.3}$$

The logarithmic derivative of the series $(b)$ is

$$\begin{aligned}\sum_{s=1}^{\infty}\frac{M_s s T^{s-1}}{1-T^s} &= T^{-1}\sum_{s=1}^{\infty}\frac{sM_sT^s}{1-T^s} \\ &= T^{-1}\sum_{s=1}^{\infty}\sum_{t=1}^{\infty}sM_sT^{st}\end{aligned}$$

while the logarithmic derivative of series $(c)$ is simply $T^{-1}\sum_{s=1}^{\infty}N_sT^s$. Comparing coefficients and using Equation 5.1.3, we find that the series $(b)$ and $(c)$ are equal. □

**Corollary 5.1.9.** *The zeta function, $Z(V,T)$ of the affine variety, $V$ over the Galois ring, $R$ has rational integer coefficients.*

To prove lemmas 5.1.5 and 5.1.6, we use Bombieri's method in generalizing Monsky's

proof of representing the zeta function $Z(V,T)$ as an *Euler product* (the series $(b)$ in the above theorem) to our situation involving $L$-functions associated to character sums over Galois rings. We will first prove the following lemma and then use the Galois theory of Galois rings to establish the lemmas stated earlier.

**Lemma 5.1.10.** *Let $R$ denote the Galois ring, $\mathbb{Z}_q/p^r\mathbb{Z}_q$ and let $P$ denote the Galois ring $\mathbb{Z}_p/p^r\mathbb{Z}_p$. Let $f$ be a polynomial in $n$ variables, $x_1, x_2, ..., x_n$ over $R$ so that its $r$-expansion is a polynomial in $nr$ variables $x_{i,j}$ obtained from the $p$-adic expansion, $x_i = x_{i,0} + x_{i,1}p + ... + x_{i,r-1}p^{r-1}$ at level $r$, for each of the $x_i$. For each positive integer $l$, let $R_l$ be the degree-$l$ Galois ring extension of $R$ and let $S_l(f) = S_l(q, r, \Theta^{(r)}, f)$ be the character sum*

$$S_l(f) = S_l(q, r, \Theta^{(r)}, f) := \sum_{x \in R_l^n} \Theta^{(r)} \circ \tau(q, l, r)(f(x))$$

*where $\Theta_r$ is the character of $P$ and $\tau(q, l, r)$ is the generalized trace map, $\mathrm{Tr}_{R_l/P}$, as defined in Chapter 2. Let $L(f, T)$ be the associated $L$-function,*

$$L(f, T) = \exp\left(\sum_{l=1}^{\infty} \frac{S_l(f)T^l}{l}\right).$$

*Then, the coefficients $A_s$ of the Taylor series of $L(f, T)$ are algebraic integers in the algebraic number field generated by a primitive $p^r$-th root of unity.*

*Proof.* We will follow Bombieri's argument closely [Bom66]. Considering the affine $n$-space, $\mathbb{A}^n(R)$, of points $x = (x_1, x_2, ..., x_n)$ defined over $R$ as an affine variety over $R$ defined by the zero polynomial, we may consider the prime 0-cycles defined over $R$. Let $\bar{R}$ denote the ring, $\mathbb{Z}_q^u/p^r\mathbb{Z}_q^{(u)}$ where $\mathbb{Z}_q^{(u)}$ is the ring of integers of the maximal unramified extension, $\mathbb{Q}_q^{(u)}$ of $\mathbb{Q}_q$ in $\bar{\mathbb{Q}}_q$. If $x = (x_1, x_2, ..., x_n) \in \mathbb{A}^n(R)$ is defined over a finite Galois ring extension of $R$, let $R_m$ be the smallest such ring of definition. Then, if $\sigma \in Gal(R_m/R)$ is the *generalized Frobenius* generator, it is easily seen that the conjugates of $x$ over $R$ under the action of the *absolute Galois group*, $Gal(\bar{R}/R)$ are given by $\sigma(x), \sigma^2(x), ..., \sigma^{m-1}(x)$. As noted earlier, $\sigma$ acts on the Teichmüller digits of

the $p$-adic representation of each component of $x$ as the $q$-power map, that is, for

$$x_i = x_{i,0} + x_{i,1}p + ... + x_{i,r-1}p^{r-1}$$

we have that

$$\sigma(x_i) = x_{i,0}^q + x_{i,1}^q p + ... + x_{i,r-1}^q p^{r-1}$$

for each $i = 1, 2, ..., n$. Then the prime $R$-rational 0-cycle associated with $x$ is denoted by $\mathfrak{p}$ and is given by

$$\mathfrak{p} = x + \sigma(x) + ... + \sigma^{m-1}(x).$$

The degree of $\mathfrak{p}$ is $\deg(\mathfrak{p}) = m$.

Now, since $f$ is defined over $R$, $\sigma$ fixes its coefficients and hence it follows that

$$\sigma(f(x)) = f(\sigma(x))$$

and hence the value of the trace $\mathrm{Tr}_{R_m/P}(f(x))$ is the same for $x$ and all of its conjugates.

(To see this, recall that if $\lambda$ is the generalized Frobenius generator of $Gal(R_m/P)$, then $\lambda$ acts on $f(y)$ (for some element $y$ in $R_m$) as the $p$-power map on the Teichmüller digits of the $p$-adic expansion at level $r$ of each of the coefficients and on those of $y$. That is, if $y = \sum_{j=0}^{r-1} y_j p^j$, then $\lambda(y) = \sum_{j=0}^{r-1} y_j^p p^j$, and if $f(y) = \sum_{u=0}^{t} a_u y^u$, the $r$-expansion of $f$ is given by

$$f(y) = \sum_{u=0}^{t} \left( \sum_{s=0}^{r-1} a_{u,s} p^s \right) \left( \sum_{j=0}^{r-1} y_j p^j \right)^u$$

and hence,

$$\begin{aligned} \lambda\left(f(y)\right) &= \sum_{u=0}^{t} \left( \sum_{s=0}^{r-1} \lambda(a_{u,s}) p^s \right) \left( \sum_{j=0}^{r-1} \lambda(y_j) p^j \right)^u \\ &= \sum_{u=0}^{t} \left( \sum_{s=0}^{r-1} a_{u,s}^p p^s \right) \left( \sum_{j=0}^{r-1} y_j^p p^j \right)^u . \end{aligned}$$

Similarly, for each $k = 1, 2, ..., m-1$, the map $\sigma^k$ acts on the Teichmüller digits as the

$q^k$-power map. Hence, we have for each $i = 0, 1, ..., am-1$ and for each $k = 1, 2, ..., m-1$,

$$\begin{aligned}\lambda^i\left(f(\sigma^k(y))\right) &= \lambda^i\left(\sigma^k\left[f(y)\right]\right) \\ &= \sum_{u=0}^{t}\left(\sum_{s=0}^{r-1}\lambda^i\sigma^k(a_{u,s})p^s\right)\left(\sum_{j=0}^{r-1}\lambda^i\sigma^k(y_j)p^j\right)^u \\ &= \sum_{u=0}^{t}\left(\sum_{s=0}^{r-1}(a_{u,s}^{q^k})^{p^i}p^s\right)\left(\sum_{j=0}^{r-1}(y_j^{q^k})^{p^i}p^j\right)^u.\end{aligned}$$

Thus, it is easily seen that

$$\mathrm{Tr}_{R_m/P}(f(\sigma^k(y))) = \sum_{i=0}^{am-1}\lambda^i\left(f(\sigma^k(y))\right) = \mathrm{Tr}_{R_m/P}(f(y))$$

for $k = 1, 2, ..., m-1$.

The argument extends in the multivariable case as well. Let $f(\mathbf{x}) = \sum_{\mathbf{u}\in Supp(f)} a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}}$ be a polynomial in $n$ variables, where $\mathbf{x} = (x_1, x_2, ..., x_n)$, $\mathbf{u} = (u_1, u_2, ..., u_n)$ and $Supp(f)$ is the collection of all exponent vectors $\mathbf{u}$ that have nonzero coefficients $a_{\mathbf{u}}$. Then the $r$-expansion of $f$ is given by

$$f(x) = \sum_{\mathbf{u}\in Supp(f)}\left(\sum_{s=0}^{r-1}a_{\mathbf{u},s}p^s\right)\prod_{i=1}^{n}\left(\sum_{j=0}^{r-1}x_{i,j}p^j\right)^{u_i}.$$

Again, for each $\ell = 0, 1, ..., am-1$ and for each $k = 1, 2, ..., m-1$, we have that

$$\begin{aligned}\lambda^\ell\left(f(\sigma^k(x))\right) &= \lambda^\ell\left(\sigma^k\left[f(x)\right]\right) \\ &= \sum_{\mathbf{u}\in Supp(f)}\left(\sum_{s=0}^{r-1}\lambda^i\sigma^k(a_{\mathbf{u},s})p^s\right)\prod_{i=1}^{n}\left(\sum_{j=0}^{r-1}\lambda^\ell\sigma^k(x_{i,j})p^j\right)^{u_i} \\ &= \sum_{\mathbf{u}\in Supp(f)}\left(\sum_{s=0}^{r-1}(a_{\mathbf{u},s}^{q^k})^{p^\ell}p^s\right)\prod_{i=1}^{n}\left(\sum_{j=0}^{r-1}(x_{i,j}^{q^k})^{p^\ell}p^j\right)^{u_i}.\end{aligned}$$

and again, it is easily seen that

$$\mathrm{Tr}_{R_m/P}(f(\sigma^k(x))) = \sum_{\ell=0}^{am-1}\lambda^\ell\left(f(\sigma^k(x))\right) = \mathrm{Tr}_{R_m/P}(f(x))$$

for $k = 1, 2, ..., m-1$.)

Thus, we may write $\mathrm{Tr}_{R_m/P}(f(\mathfrak{p}))$ to denote $\mathrm{Tr}_{R_m/P}(f(y))$ for any $y$ in the orbit of $x$ under the action of $Gal(\bar{R}/R)$. We immediately have the *Euler product* formula:

$$\boxed{L(f,T) = \prod_{\mathfrak{p}} (1 - \Theta^{(r)} \circ \mathrm{Tr}_P \left[f(\mathfrak{p})\right] T^{\deg(\mathfrak{p})})^{-1}} \tag{5.1.4}$$

where the product runs over all prime $R$-rational 0-cycles $\mathfrak{p}$ of $\mathbb{A}^n(R)$ and $\mathrm{Tr}_P$ denotes the *absolute* trace $\mathrm{Tr}_{R_{\deg(\mathfrak{p})}/P}$.

(To see this, we compare the coefficients of the formal logarithmic derivative of the series on the left and that on the right. The logarithmic derivative of the series on the left gives

$$T^{-1} \sum_{l=1}^{\infty} S_l(f) T^l$$

and the series on the logarithmic derivative of the series on the right gives

$$T^{-1} \sum_{d=1}^{\infty} \sum_{\substack{\mathfrak{p}: \\ \deg(\mathfrak{p})=d}} \sum_{k=1}^{\infty} d \left(\Theta^{(r)} \circ \mathrm{Tr}_{R_d/P} \left[f(\mathfrak{p})\right]\right)^k T^{dk}$$

The coefficient of $T^{l-1}$ for the above series (observe that there is a factor of $T^{-1}$ on the outside) is thus given by

$$\begin{aligned}
\sum_{d|l} \sum_{\substack{\mathfrak{p}: \\ \deg(\mathfrak{p})=d}} d \cdot \left(\Theta^{(r)} \circ \mathrm{Tr}_{R_d/P} \left[f(\mathfrak{p})\right]\right)^{l/d} &= \sum_{d|l} \sum_{\substack{\mathfrak{p}: \\ \deg(\mathfrak{p})=d}} d \cdot \left(\Theta^{(r)} \circ \mathrm{Tr}_{R_d/P} \left[\left(\frac{l}{d}\right) f(\mathfrak{p})\right]\right) \\
&= \sum_{d|l} \sum_{\substack{\mathfrak{p}: \\ \deg(\mathfrak{p})=d}} d \cdot \left(\Theta^{(r)} \circ \mathrm{Tr}_{R_l/P} \left[f(\mathfrak{p})\right]\right) \\
&= \sum_{d|l} \sum_{\substack{\mathfrak{p}: \\ \deg(\mathfrak{p})=d}} \sum_{x \in \mathfrak{p}} \Theta^{(r)} \circ \mathrm{Tr}_{R_l/P} \left[f(x)\right] \\
&= \sum_{x \in R_l} \Theta^{(r)} \circ \tau(q,l,r) \left[f(x)\right] \\
&= S_l(f).
\end{aligned}$$

where the first equality is due to the fact that $\Theta^{(r)} \circ \mathrm{Tr}_{R_d/P}$ is an additive character, and the penultimate inequality is by the Galois theory of Galois rings (from which we obtained Equation 5.1.3 earlier).

).

From Equation 5.1.4, it is clear that the coefficients of $L(f,T)$ are algebraic integers in the algebraic number field generated by a primitive $p^r$-th root of unity. □

Now, in order to prove Lemma 5.1.6, we first observe the following fact.

**Definition 5.1.11.** Let $R$ be the Galois ring of characteristic $p^r$ and cardinality $q^r$. (We identify $R$ with the ring $\mathbb{Z}_q/p^r\mathbb{Z}_q$). Let $\bar{R}$ denote the ring $\mathbb{Z}_q^{(u)}/p^r\mathbb{Z}_q^{(u)}$. For each integer $l$, let $R_l$ denote the degree-$l$ Galois ring extension of $R$. Let $A$ be a subset of $J_r := \{0,1,2,...,r-1\}$. For each $l$, we define the subset $R_l^A$ to be

$$R_l^A := \left\{ x = x_0 + x_1 p + ... + x_{r-1}p^{r-1} \in R_l : \begin{cases} x_i \neq 0, & \text{if } i \in A \\ x_i = 0, & \text{if } j \notin A \end{cases} \right\}.$$

**Lemma 5.1.12.** *With the above definition, for any subset $A \in J_r$ and any positive integer $l$, if $x \in R_l^A$, then all of its Galois conjugates over $R$ belong to $R_l^A$ as well.*

*Proof.* This is clear from the fact that if $\sigma \in Gal(R_l/R)$ is the generalized Frobenius generator, then

$$\sigma(x_0 + x_1 p + ... + x_{r-1}p^{r-1}) = x_0^q + x_1^q p + ... + x_{r-1}^q p^{r-1}.$$

□

**Corollary 5.1.13.** *Let $R$ be the Galois ring of characteristic $p^r$ and cardinality $q^r$. (We identify $R$ with the ring $\mathbb{Z}_q/p^r\mathbb{Z}_q$). Let $\bar{R}$ denote the ring $\mathbb{Z}_q^{(u)}/p^r\mathbb{Z}_q^{(u)}$. Let $\mathbb{A}^n(R)$ denote the affine $n$-space over $R$ consisting of points $x = (x_1, x_2, ..., x_n)$. We may identify $\mathbb{A}^n(R)$ with the affine variety (defined by the zero polynomial) consisting of all of its $\bar{R}$-rational points.*

*Let $x$ be a point of $\mathbb{A}^n(R)$. Let $l$ be the smallest positive integer such that $x \in R_l^n$. For each $i = 1,2,...,n$, let $A_i$ be a subset of $J_r := \{0,1,2,...,r-1\}$. If for each $i = 1,2,...,n$,*

$x_i \in R_l^{A_i}$, *then all the points in the orbit of* $x$ *under the action of* $Gal(\bar{R}/R)$ *are in* $\prod_{i=1}^{n} R_l^{A_i}$.

*Proof.* This follows from the previous lemma. □

We can now prove Lemma 5.1.6 from which Lemma 5.1.5 follows.

*Proof of Lemma 5.1.6.* We may repeat the argument in Lemma 5.1.10 and observe that due to Corollary 5.1.13, the $L$-function now has an Euler product expansion

$$L(f,T) = \prod_{\mathfrak{p}}{}' (1 - \Theta^{(r)} \circ \mathrm{Tr}_P \left[f(\mathfrak{p})\right] T^{\deg(\mathfrak{p})})^{-1} \tag{5.1.5}$$

where the product $\prod_{\mathfrak{p}}{}'$ runs over all prime 0-cycles $\mathfrak{p}$ such that if $\mathfrak{p} = x + \sigma(x) + ... + \sigma^{m-1}(x)$ and $x = (x_1, x_2, ..., x_n)$, then for all $i = 1, 2, ..., n$, $x_i \in R_m^{A_i}$. □

We can now, finally, establish the rationality of our $L$-function.

**Theorem 5.1.14.** *The L-function that we considered in this thesis,* $L^*(\bar{f}, T)$*, is a rational function of* $T$.

*Proof.* By Lemma 5.1.2 (or by the stronger Lemma 5.1.5), Dwork's rationality criterion (Theorem 5.1.1) is applicable to the $L$-function. By Lemma 5.1.5, condition $(i)$ in Theorem 5.1.1 is satisfied by $L^*(\bar{f}, T)$. In fact, $|A_s|_v \leq 1$ for *all* finite primes $v$. By Lemma 5.1.3 and Lemma 5.1.4, condition $(ii)$ in Theorem 5.1.1 is satisfied. Hence, $L^*(\bar{f}, T)$ is rational. □

**Remark 5.1.15.** Before we proceed to the next section, it is worthwhile to make the following observations. We had considered several related $L$-functions and the *zeta function* of an affine variety over a Galois ring in this section in order to establish the rationality of our $L$-function. We may imitate our arguments and similarly establish the rationality of the other $L$-functions as well. The analogues of Lemma 5.1.4 are easily proven. These along with Lemma 5.1.6, just leave us with establishing analogues for Lemma 5.1.3 in order to prove the rationality using Dwork's criterion. This requires

us to prove analogous trace formulas for the respective sequences of exponential sums corresponding to the respective $L$-function. Such Dwork trace formulas can, in principle, be proven by using the diagrammatic weight function that we constructed in Chapter 3. Having established the rationality of all these related $L$-functions, the rationality of the *zeta function* follows from a simple combinatorial argument.

## 5.2 Bombieri-Adolphson-Sperber Bounds on the Degree of the $L$-function

Another important application of the trace formula and the associated $p$-adic theory is to obtain estimates on the degree and the total degree of the $L$-function (once it is known that the $L$-function is rational) following Bombieri's argument in [Bom66] and [Bom78] and related arguments in [AS87a] which improve the basic estimates of Bombieri. Once we establish the rationality of the $L$-function, we may define its *degree* to be the integer $R-S$ where $R$ is the number of its zeros and $S$ is the number of its poles. And similarly, we may also define its *total degree* to be the integer $R+S$.

In what follows, we will prove the analogue of Bombieri-Adolphson-Sperber estimate for the degree $(R-S)$ of our $L$-function (or its reciprocal). We will present the argument in four steps as follows.

**Step 1**

We recall that our $L$-functon is related to the associated Fredholm determinant in terms of the Dwork's $\delta$-operator given by Theorem 4.1.5:

$$L^*(\bar{f},T) = L^*(q,r,\Theta_r,\bar{f},T)^{(-1)^{(N+1)}} = \det(\mathbb{I}-\alpha T)^{\delta^N} \tag{5.2.1}$$

where

$$\boxed{P(t)^{\delta} := \frac{P(t)}{P(qt)}}$$

for a rational function or Laurent series $P(t) \in K((t))$ and $\boxed{N = nr}$ is the total number of variables at level $r$. Bombieri exploits the fact that $\det(\mathbb{I} - \alpha T)$ is a $p$-adically entire function by first rewriting Equation 5.2.1 as

$$\left[L^*(\bar{f}, T)^{(-1)^{N+1}}\right]^{\delta^{-N}} = \det(\mathbb{I} - \alpha T) \tag{5.2.2}$$

and then obtaining an expression for the left hand side as follows. Like the $\delta$ operator, Dwork also defines the $\phi$ operator (with respect to $q$) defined on any rational function of Laurent series, $P(t) \in \mathbb{C}_p((t))$ by $P(t)^{\phi} = P(qt)$. Then clearly $\delta = 1 - \phi$, where 1 represents the identity map. And thus

$$\delta^{-N} = (1 - \phi)^{-N} = \sum_{j=0}^{\infty} c(j)\phi^j$$

where the $c(j)$ are the binomial coefficients $\binom{N+j-1}{N-1}$. Now since $L^*(\bar{f}, T)$ is a rational function in $1 + T\mathbb{C}_p[[T]]$, we may write

$$L^*(\bar{f}, T)^{(-1)^{N+1}} = \frac{\prod_{h=1}^{R}(1 - \omega_h T)}{\prod_{j=1}^{S}(1 - \eta_j T)}$$

where $\omega_h^{-1}$ and $\eta_j^{-1}$ are zeros and poles (respectively) of $L^*(\bar{f}, T)^{(-1)^{N+1}}$ for some positive integers $R$ and $S$. Hence, Equation 5.2.2 becomes

$$\left[\frac{\prod_{h=1}^{R}(1 - \omega_h T)}{\prod_{j=1}^{S}(1 - \eta_j T)}\right]^{\sum_{j=0}^{\infty} c(j)\phi^j} = \det(\mathbb{I} - \alpha T)$$

which can be rewritten as

$$\det(\mathbb{I} - \alpha T) = \frac{D_1(T)}{D_2(T)} \tag{5.2.3}$$

where

$$D_1(T) = \prod_{h=1}^{R}\prod_{i=0}^{\infty}(1-\omega_h q^i T)^{c(i)}, \text{ and } D_2(T) = \prod_{j=1}^{S}\prod_{i=0}^{\infty}(1-\eta_j q^i T)^{c(i)}.$$

For the case when $r = 1$, a simple argument as a consequence of ([Bom66]: Lemma 1) where he shows that the coefficients of the Taylor series of $L^*(\bar{f}, T)$ are algebraic integers in $\mathbb{Q}(\zeta_{p^r})$, along with Krasner's theorem on the uniqueness of analytic continuation shows that the $\omega_h$ and the $\eta_j$ are algebraic integers.

For the general case when $r > 1$, we can use the same argument involving the use of Krasner's Theorem, having established the analogous Lemma 5.1.5. We could also use the following argument based on an exercise in [Kob84] instead to deduce that $\omega_h$ and $\eta_j$ are algebraic integers.

We recall that the **$p$-adic Gauss norm** of a polynomial or a power series with coefficients in $\mathbb{C}_p$ is the supremum of the $p$-adic absolute values of the coefficients. If $g(t)$ is in $\mathbb{C}_p[[t]]$ or $\mathbb{C}_p[t]$, let us denote its $p$-adic Gauss norm by $|g|_p$.

**Lemma 5.2.1.** *If $g(t) = \dfrac{h(t)}{f(t)}$ is a power series in $1 + t\mathbb{C}_p[[t]]$ with $h(t)$ and $f(t)$ being polynomials with no common factors, factored in terms of reciprocal zeros as*

$$h(t) = \prod_{i=1}^{R}(1-\alpha_i t)$$

*and*

$$f(t) = \prod_{j=1}^{S}(1-\beta_j t),$$

*and if the coefficients of $g(t)$ are in the $p$-adic unit disk (that is, their absoulute values are less than or equal to one), then the $\alpha_i$ and the $\beta_j$ are also in the $p$-adic unit disk.*

*Proof.* Let us first rewrite $h(t)$ and $f(t)$ as

$$h(t) = 1 + \sum_{i=1}^{k} h_i t^i$$

and

$$f(t) = 1 + \sum_{j=1}^{\ell} f_j t^j$$

by expanding them out. We will now use a Gauss norm argument to show that the the $h_i$ and the $f_j$ are in the $p$-adic unit disk. Since $|g|_p = 1$, we have that

$$|g|_p = \frac{|h|_p}{|f|_p} = 1.$$

We claim that $|h|_p = 1$ and $|f|_p = 1$. To see this, we first write $\hat{f}(t) = \frac{1}{f(t)}$ as

$$\hat{f}(t) = 1 + \sum_{j=1}^{\infty} \hat{f}_j t^j$$

and we see that

$$|g|_p = |h\hat{f}|_p = 1.$$

Suppose for the sake of contradiction that $|h|_p > 1$ or $|f|_p > 1$. Note that if $|f|_p > 1$, then $|\hat{f}|_p > 1$ as well. Let $m$ be the the smallest integer such that $|h_m|_p = \max\{|h_i|_p : i = 0, 1, \ldots, k\}$, and let $n$ be the smallest integer such that $|\hat{f}_n|_p = \max\{|\hat{f}_j|_p : j = 0, 1, 2, \ldots\}$.

Now consider the coefficient of $t^{m+n}$ in the expansion of $h(t)\hat{f}(t)$. Then, by definition of $m$ and $n$, it follows that the absolute value of the coefficient is $|h_m\hat{f}_n|$. This is because this coefficient is the sum of $h_i\hat{f}_j$ over $i + j = m + n$. But then the term with uniquely maximum absolute value is the one with $i = m$ and $j = n$ since all other terms have a factor $h_i$ or $\hat{f}_j$ with index $i < m$ or $j < n$, so has absolute value strictly less than $|h_m\hat{f}_n|$.

From aove, it follows that if $|h|_p > 1$ or $|f|_p > 1$, then $|g|_p > 1$, a contradiction. Thus, $|h|_p = 1$ and $|f|_p = 1$.

Now rearrange the $\alpha_i$ in the increasing order of absolute values so that $|\alpha_1| \leq |\alpha_2| \leq \ldots \leq |\alpha_R|$. Let $s$ be the largest integer such that $|\alpha_s| \leq 1$. Then consider the coefficient of $t^{R-s}$ in the expansion of $h(t) = \prod_{i=1}^{R}(1 - \alpha_i t)$. The term $\alpha_{s+1}\alpha_{s+2}\ldots\alpha_R$ in this coefficient has the maximum absloute value and is equal to the the absolute value of this coefficient, which is greater than one contradicting the above conclusion that $|h|_p = 1$

unless $s = R$. Thus, all the $\alpha_i$ are in the $p$-adic unit disk.

By a very similar argument, all the $\beta_j$ are also in the $p$-adic unit disk. □

**Theorem 5.2.2.** *The $\omega_h$ and the $\eta_j$ in the above expression for $L^*(\bar{f}, T)^{(-1)^{N+1}}$ are algebraic integers.*

*Proof.* The previous lemma can be applied to $L^*(\bar{f}, T)^{(-1)^{N+1}}$ due to Lemma 5.1.5 and the easily proven fact that if $g(T) \in 1 + TO_K[[T]]$ where $O_K$ is the ring of integers of an algebraic number field $K$, then $1/g(T) \in 1 + TO_K[[T]]$ as well.

From the lemma, it follows that the $\omega_h$ and the $\eta_j$ are in the $p$-adic unit disk. By repeating the argument in the previous lemma for all finite primes, $\ell$, it follows that $|\omega_h|_\ell \leq 1$ and $|\eta_j|_\ell \leq 1$ for all finite primes $\ell$ for $1 \leq h \leq R$ and $1 \leq j \leq S$. It follows that the $\omega_h$ and the $\eta_j$ are algebraic integers by a standard theorem in number theory. □

Now, since the left hand side of Equation 5.2.3 is entire, it follows that all the zeros of $D_2(T)$ must cancel with the zeros of $D_1(T)$. A straightforward argument using this fact shows that $R - S \geq 0$ and if $S \geq 1$, then for each $j \in \{1, 2, ..., S\}$, $\eta_j = q^{b_h}\omega_h$ for some $h \in \{1, 2, ..., R\}$ and some nonzero integer $b_h$.

**Step 2**

Next, Bombieri uses Dwork's arguments [Dwo64] to obtain an estimate on the Newton polygon of $\det(\mathbb{I} - \alpha T)$ as follows. Here, let $\boxed{K_q = \mathbb{Q}_q(\zeta_{p^r})}$ and let $\boxed{K_p = \mathbb{Q}_p(\zeta_{p^r})}$. Let $\mathrm{ord}_q$ denote the valuation on $\mathbb{C}_p$ normalized by $\mathrm{ord}_q\, q = 1$. And thus, $\mathrm{ord}_p = a\,\mathrm{ord}_q$. Let $\sigma$ be the Frobenius generator of $Gal(K_q/K_p)$. Then, we recall (from the previous chapter) that the map $\alpha$ decomposes as $\alpha_0^a$ where $\alpha_0 = i_p \circ \sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x})$. We observed that even though $\alpha_0$ is not $K_q$-linear, it is $K_p$-linear. And in fact, as a $K_p$-linear endomorphism of the space $B_{\bar{f}}\left(\dfrac{p}{q(p-1)}\right)$, we have that $\alpha = \alpha_0^a$.

Now, since $\alpha$ is both a $K_q$-linear and a $K_p$-linear endomorphism of $B_{\bar{f}}\left(\dfrac{p}{q(p-1)}\right)$,

the characteristic polynomial $\det(\mathbb{I}-\alpha T)$ has different meanings depending on the choice of the field over which the Banach space $B_{\bar{f}}\left(\frac{p}{q(p-1)}\right)$ is defined. Using subscripts to denote the choice of the field, Dwork observes that

$$\det_{K_p}(\mathbb{I}-\alpha T) = N_{K_q/K_p} \det_{K_q}(\mathbb{I}-\alpha T)$$

with the norm being interpreted in the sense of products of conjugates of $K_q$ over $K_p$, the automorphisms acting trivially on the variable $T$.

Now, on one hand, we have, by the theory of characteristic polynomials, that

$$\det_{K_p}(\mathbb{I}-\alpha_0^a T^a) = \prod_{\lambda} \det_{K_p}(\mathbb{I}-\alpha_0(\lambda T)) \tag{5.2.4}$$

where the product runs over all $\lambda$ satisfyting $\lambda^a = 1$. On the other hand, from Theorem 5.2.2, the coefficients of the Taylor series of $L^*(\bar{f},T)$ lie in the algebraic number field, $\mathbb{Q}(\zeta_{p^r}) \subset K_p$, and thus $\det_{K_q}(\mathbb{I}-\alpha T) \in K_p[[T]]$. And therefore, the conjugates of $\det_{K_q}(\mathbb{I}-\alpha T)$ are all equal and from Dwork's observation we have that

$$\det_{K_p}(\mathbb{I}-\alpha T) = \det_{K_q}(\mathbb{I}-\alpha T)^a$$

and similarly,

$$\begin{aligned}\det_{K_p}(\mathbb{I}-\alpha T^a) &= N_{K_q/K_p} \det_{K_q}(\mathbb{I}-\alpha T^a) \\ &= \left[\det_{K_q}(\mathbb{I}-\alpha T^a)\right]^a . \end{aligned} \tag{5.2.5}$$

Hence, from equations 5.2.4 and 5.2.5 and from the fact that $\alpha_0^a = \alpha$, we deduce that

$$\left[\det_{K_q}(\mathbb{I}-\alpha T^a)\right]^a = \prod_{\lambda^a=1} \det_{K_p}(\mathbb{I}-\alpha_0(\lambda T)). \tag{5.2.6}$$

The above equation helps us to compute the Newton polygon of $\det_{K_q}(\mathbb{I}-\alpha T)$ in terms of that of $\det_{K_p}(\mathbb{I}-\alpha_0 T)$. More precisely, Dwork shows ([Dwo64]: Lemma 7.1) that a point $(x,y) \in \mathbb{R}^2$ is a vertex in the Newton polygon of $\det_{K_q}(\mathbb{I}-\alpha T)$ computed

with respect to the valuation $\mathrm{ord}_q$ if and only if the point $(ax, ay)$ is a vertex of the Newton polygon of $\det_{K_p}(\mathbb{I} - \alpha_0 T)$ computed with respect to the valuation $\mathrm{ord}_p$. Thus it suffices to estimate the Newton polygon of $\det_{K_p}(\mathbb{I} - \alpha_0 T)$.

In order to estimate the Newton polygon of $\det_{K_p}(\mathbb{I} - \alpha_0 T)$, we first consider $K_q$ as a $K_p$-vector space of dimension $a$ and we may choose an integral basis $\{\xi_1, \xi_2, ..., \xi_a\}$ of $K_q$ over $K_p$ such that $K_q$ is a $p$-adically direct sum of $a$ copies of $K_p$ ([Dwo62]: Section $3(c)$) with respect to this basis. That is, for every $\beta_1, \beta_2, ..., \beta_a \in K_p$,

$$\mathrm{ord}_p \left( \sum_{i=1}^{a} \beta_i \xi_i \right) = \min_i \mathrm{ord}_p \, \beta_i$$

It can be shown that such a basis exists. Now, the collection $\{\xi_i \mathbf{x}^u : u \in \mathbb{Z}_{\geq 0}^N, i = 1, 2, ..., a\}$ forms a $K_p$-basis for the $p$-adic Banach space, $B_{\bar{f}}\left(\frac{p}{q(p-1)}\right)$. Now, writing $F_{0,0}(\mathbf{x}) = \sum_u a_u \mathbf{x}^u$, for some coefficients $a_u \in K_q$, we may express these coefficients as

$$a_u = \sum_{k=1}^{a} a_{u,k} \xi_k$$

for some $a_{u,k} \in K_p$ in terms of the basis $\{\xi_1, ..., \xi_a\}$. Similarly, we may express $\sigma^{-1}(\xi_j \xi_k)$ as

$$\sigma^{-1}(\xi_j \xi_k) = \sum_{i=1}^{a} s_{ijk} \xi_i$$

for some $s_{ijk} \in K_p$. Then since, $\mathrm{ord}_p \, \xi_i = 0$ for all $i$, it follows that $\mathrm{ord}_p \, \sigma^{-1}(\xi_j \xi_k) \geq 0$ and hence $\mathrm{ord}_p \, s_{ijk} \geq 0$. Also, since $F_{0,0}(\mathbf{x}) \in B_{\bar{f}}\left(\frac{1}{p-1}\right)$, we have

$$\mathrm{ord}_p \, a_u \geq \frac{w_\Sigma(u)}{(p-1)}$$

and thus

$$\mathrm{ord}_p \, a_{u,k} \geq \frac{w_\Sigma(u)}{(p-1)}$$

Then for a generic element $\sum_u \left( \sum_{i=1}^{a} c_{u,i} \xi_i \right) \mathbf{x}^u$ (with the $c_{u,i} \in K_p$) of $B_{\bar{f}}\left(\frac{p}{q(p-1)}\right)$,

the $K_p$-linear map $\alpha_0 = i_p \circ \sigma^{-1} \circ \psi_p \circ F_{0,0}(\mathbf{x})$ acts by

$$c_{u,i} \mapsto \sum_v \sum_{k=1}^{a} a_{pu-v,k} s_{ijk} c_{v,j}$$

and thus we obtain a matrix representation $(A_{u,i;v,j})$ of $\alpha_0$ given by

$$A_{u,i;v,j} = \sum_{k=1}^{a} a_{pu-v,k} s_{ijk}.$$

Then it follows from the above arguments that $A_{u,i;v,j} = 0$ when the $n$-uple $pu - v$ contains a negative element, and

$$\operatorname{ord}_p A_{u,i;v,j} \geq \frac{w_\Sigma(pu - v)}{(p-1)}$$

otherwise.

On the other hand, writing

$$\det_{K_p}(\mathbb{I} - \alpha_0 T) = \sum_{m-0}^{\infty} b_m T^m$$

and setting $A(u,i;v,j) = A_{u,i;v,j}$ we observe that the coefficients $b_m$ are given by

$$b_m = \sum \pm \prod_{\nu=1}^{m} A(u_\nu, i_\nu; v_\nu, j_\nu)$$

where the sum is over all sets of $m$ 4-uples $(u_\nu, i_\nu, v_\nu, j_\nu)$ such that the $m$ pairs $(u_\nu, i_\nu)$ are distinct and the $m$ pairs $(v_\nu, j_\nu)$ are permutations of the $m$ pairs $(u_\nu, i_\nu)$, and the signs in the sum are determined by $m$ and the signature of the permutation. Then, we have that

$$\operatorname{ord}_p b_m \geq \min \sum_{\nu=1}^{m} \frac{w_\Sigma(pu_\nu - v_\nu)}{(p-1)}$$

where the minimum is taken over all $m$ quadruplets as described above.

Also, by the convexity of the weight function, $w_\Sigma$, we have that

$$\sum_{\nu=1}^{m} w_\Sigma(pu_\nu) \leq \sum_{\nu=1}^{m} w_\Sigma(pu_\nu - v_\nu) + \sum_{\nu=1}^{m} w_\Sigma(v_\nu)$$

and thus,

$$\begin{aligned} p\sum_{\nu=1}^{m} w_\Sigma(u_\nu) - \sum_{\nu=1}^{m} w_\Sigma(v_\nu) &\leq \sum_{\nu=1}^{m} w_\Sigma(pu_\nu - v_\nu) \\ \implies (p-1)\sum_{\nu=1}^{m} w_\Sigma(u_\nu) &\leq \sum_{\nu=1}^{m} w_\Sigma(pu_\nu - v_\nu) \end{aligned}$$

whence

$$\operatorname{ord}_p b_m \geq \min \sum_{\nu=1}^{m} \frac{w_\Sigma(pu_\nu - v_\nu)}{(p-1)} \geq \min \sum_{\nu=1}^{m} w_\Sigma(u_\nu)$$

where the first minimum is taken over all $m$ quadruplets as described above and the second minimum is taken over all $m$ distinct pairs $(u_\nu, i_\nu)$.

Hence, the Newton polygon of $\det_{K_p}(\mathbb{I} - \alpha_0 T)$, which is the convex closure of the points $(m, \operatorname{ord}_p b_m)$ is contained in the convex closure of the points

$$\left(m, \min \sum_{\nu=1}^{m} w_\Sigma(u_\nu)\right) \tag{5.2.7}$$

where the minimum is again taken over all $m$ distinct pairs $(u_\nu, i_\nu)$.

Thus, as described in [AS87a], the problem of estimating the Newton polygon of the series, $\det_{K_p}(\mathbb{I} - \alpha_0 T)$ reduces to the problem of counting the number of $u \in \mathbb{Z}^N$ of a given weight. Since our weight function $w_\Sigma$ satisfies Proposition 3.2.22 analogous to Lemma 2.14 in [AS87a], we may define integers $W(j)$ for $j = 0, 1, 2, ...$ by

$$W(j) = \operatorname{card}\left\{u \in \mathbb{Z}^N : w_\Sigma(u) = \frac{j}{D}\right\}$$

where $D$ is the smallest positive integer such that $w_\Sigma(\mathbb{Z}^N) \subseteq \frac{1}{D}\mathbb{Z}_{\geq 0} \cup \{+\infty\}$ where $\mathbb{Z}_{\geq 0}$ denotes the set of all nonnegative integers.

Then, following [AS87a], we note that from a simple combinatorial argument ([Dwo64]: Section 7), it follows that the convex closure of the points given by (5.2.7) above coincides with the convex closure of the points

$$\left( a\sum_{j=0}^{M} W(j), \frac{a}{D}\sum_{j=0}^{M} jW(j) \right), \qquad M = 0, 1, 2, \ldots.$$

along with $(0, 0)$. Finally, from the paragraph following Equation 5.2.6, we have an estimate for the Newton polygon of $\det_{K_q}(\mathbb{I} - \alpha T)$ with respect to the valuation $\mathrm{ord}_q$ given by the convex closure of the points

$$\left( \sum_{j=0}^{M} W(j), D^{-1}\sum_{j=0}^{M} jW(j) \right), \qquad M = 0, 1, 2, \ldots$$

along with $(0, 0)$.

**Step 3**

Next, Bombieri proves a $p$-adic analogue of Jensen's formula for entire functions using the theory of Newton polygons and uses this to obtain a result useful for our estimation. This result is later generalized by Adolphson and Sperber [[AS87a]: Lemma 4.2]. More precisely, for our situation, we have the following lemma [[Bom66]] and corollary [[AS87a]].

**Lemma 5.2.3.** *Let $D(t) = 1 + \sum_{j=1}^{\infty} d_j t^j$ be an entire function in $\mathbb{C}_p$, and let $\{\rho_i\}$ be the sequence of reciprocals of the zeros of $D(t)$ ordered such that $\mathrm{ord}_p \rho_i \leq \mathrm{ord}_p \rho_{i+1}$ for all $i$. Then we have for every real $x$*

$$\sum (x - \mathrm{ord}_p \rho_i) = \max_{j \geq 0}(xj - \mathrm{ord}_p d_j)$$

*where the sum is over all $i$ such that $\mathrm{ord}_p \rho_i \leq x$.*

And the lemma above also holds when $\mathrm{ord}_p$ is replaced by $\mathrm{ord}_q$. Also, it suffices to consider only the integers $j$ such that $(j, \mathrm{ord}_q d_j)$ is a vertex of the Newton polygon of $D(t)$ when taking the maximum in the above lemma. Applying the lemma to the

entire function $\det_{K_q}(\mathbb{I} - \alpha T)$, and using Equation 5.2.3 and the bounds on the Newton polygon of $\det_{K_q}(\mathbb{I} - \alpha T)$ obtained in Step 2, we get

**Corollary 5.2.4.** *For every real $x \geq 0$,*

$$\sum_{h=1}^{R}{\sum}'(x-\mathrm{ord}_q(q^i\omega_h))c(i)-\sum_{j=1}^{S}{\sum}'(x-\mathrm{ord}_q(q^i\eta_j))c(i) \leq x\sum_{k\leq Dx}W(k)-D^{-1}\sum_{k\leq Dx}kW(k) \tag{5.2.8}$$

*where the sums $\sum'$ are over all $i$ such that the summands are positive, and $c(i) = \binom{i+N-1}{N-1}$.*

**Step 4**

In the last step, we observe the following asymptotic relationship:

**Lemma 5.2.5.**

$$\sum_{i\leq x}(x-i)c(i) = \frac{x^{N+1}}{(N+1)!} + O(x^N) \tag{5.2.9}$$

*where the sum runs over all nonnegative integers $i$ less than or equal to a fixed nonnegative real number $x$.*

Then, on one hand, fixing $h \in \{1, 2, ..., R\}$, we observe that

$$\begin{aligned}\sum{}'(x - \mathrm{ord}_q(q^i\omega_h))c(i) &= \sum_{i\leq x-\mathrm{ord}_q\,\omega_h}\left[(x-\mathrm{ord}_q\,\omega_h)-i\right]c(i)\\ &= \frac{(x-\mathrm{ord}_q\,\omega_h)^{N+1}}{(N+1)!} + O(x^N)\end{aligned}$$

where $\sum'$ is as defined in Corollory 5.2.4 and the second sum runs over all nonnegative integers $i$ satisfying $i \leq x - \mathrm{ord}_q\,\omega_h$. The second equality follows from Lemma 5.2.9. Repeating this argument for each $\omega_h$ and each $\eta_j$ we get

$$\boxed{\sum_{h=1}^{R}{\sum}'(x-\mathrm{ord}_q(q^i\omega_h))c(i) - \sum_{j=1}^{S}{\sum}'(x-\mathrm{ord}_q(q^i\eta_j))c(i) = (R-S)\left[\frac{x^{N+1}}{(N+1)!}\right] + O(x^N)}. \tag{5.2.10}$$

On the other hand, we can obtain an asymptotic expression in terms of the $\Sigma$-diagram of the polynomial $\bar{f}$ for the right hand side of Equation 5.2.8 by following the

arguments in [AS87a] as described below, we will be able to prove the following result.

**Theorem 5.2.6.** *Let $E(\bar{f})$ be the smallest subspace of $\mathbb{R}^N$ containing $\Sigma(\bar{f}, r)$, the level-$r$ $\Sigma$-diagram of $\bar{f}$. Let $\tilde{N}$ be the dimension of $E(\bar{f})$. (Note that $\tilde{N} \leq N$ with equality holding in most generic cases). Let $\tilde{V}(\bar{f})$ be the $\tilde{N}$-dimensional volume of $\Sigma(\bar{f}, r)$ with respect to the Haar measure on $E(\bar{f})$ normalized so that a fundamental domain for the lattice $E(\bar{f}) \cap \mathbb{Z}^N$ has volume 1.*

*Then with the notations used in this section, we have*

*(a)*

$$x \sum_{k \leq Dx} W(k) = \tilde{V}(\bar{f}) x^{\tilde{N}+1} + O(x^{\tilde{N}}).$$

*(b)*

$$D^{-1} \sum_{k \leq Dx} kW(k) = \frac{\tilde{N}\tilde{V}(\bar{f})}{\tilde{N}+1} x^{\tilde{N}+1} + O(x^{\tilde{N}}).$$

Equation 5.2.10 and the above theorem give asymptotic growth for the left hand side and the right hand side of Corollary 5.2.4. Using these, we have

$$\boxed{(R-S)\left[\frac{x^{N+1}}{(N+1)!}\right] + O(x^N) \leq \frac{\tilde{N}!\tilde{V}(\bar{f})}{(\tilde{N}+1)!} x^{\tilde{N}+1} + O(x^{\tilde{N}})}$$

Now, if $\tilde{N} = N$, then we identify $\tilde{V}(\bar{f})$ with $V(\bar{f})$, defined as the volume of $\Sigma(\bar{f}, r)$ with respect to the Lebesgue measure on $\mathbb{R}^N$.

Letting $x \to \infty$, we see that if $\boxed{\tilde{N} = N}$, then

$$\boxed{(R-S) \leq N!V(\bar{f})} \tag{5.2.11}$$

and if $\tilde{N} < N$, then $(R-S) \leq 0$, and also, from the paragraph following Theorem 5.2.2, we also have that $(R-S) \geq 0$. We have thus obtained the Bombieri-Adolphson-Sperber estimate on the degree of our $L$-function. We have

**Theorem 5.2.7.** *With the notations used in this section, we have that*

*(a) If $\tilde{N} = N$, then*

$$\boxed{0 \leq \textit{degree } L^*(\bar{f}, T)^{(-1)^{N+1}} = (R - S) \leq N! V(\bar{f})}.$$

*(b) If $\tilde{N} < N$, then*

$$\boxed{\textit{degree } L^*(\bar{f}, T)^{(-1)^{N+1}} = (R - S) = 0}.$$

In the following subsection we will prove Theorem 5.2.6.

### 5.2.1 Proof of Theorem 5.2.6

We will follow the arguments in [AS87a] closely.

Let $r \geq 2$. A "face" of $\Sigma(\bar{f}, r)$ means a closed face of arbitrary dimension. For each face $\Gamma$ of $\Sigma(\bar{f}, r)$, let $C(\Gamma)$ be the union of all half-lines emenating from the origin and passing through $\Gamma$. Let $\hat{\Gamma}$ be the convex hull of $\Gamma \cup \{(0, 0, ..., 0)\}$. Let $\tilde{V}(\Gamma)$ (resp. $\tilde{V}(\hat{\Gamma})$) be the volume of $\Gamma$ (resp. $\hat{\Gamma}$) with respect to the Haar measure on the smallest affine space (resp. linear space) containing $\Gamma$ (resp. $\hat{\Gamma}$), normalized so that a fundamental domain for the induced lattice has volume 1. Let $E(\bar{f})$ be the smallest subspace of $\mathbb{R}^N$ containing $\Sigma(\bar{f}, r)$ and set $\tilde{N} = \dim E(\bar{f})$.

Now, let $\Gamma$ be an $(\tilde{N}-1)$-dimensional face of $\Sigma(\bar{f}, r)$. Defining $W_\Gamma(j)$ for $j = 0, 1, 2, ...,$ by

$$W_\Gamma(j) = \text{card} \left\{ u \in \mathbb{Z}^N \cap C(\Gamma) : w_\Sigma(u) = \frac{j}{D} \right\}$$

and $D(\Gamma)$ to be the smallest positive integer such that

$$w_\Sigma \left( \mathbb{Z}^N \cap C(\Gamma) \right) \subseteq \frac{1}{D(\Gamma)} \mathbb{Z}_{\geq 0} \cup \{+\infty\}$$

the argument in [AS87a] that uses Ehrhart's Corollary 4.2.3 [Ehr67] gives the asymptotic estimate

$$W_\Gamma(j) = \frac{\tilde{V}(\Gamma)}{D(\Gamma)^{\tilde{N}-1}} (j')^{\tilde{N}-1} + O((j')^{\tilde{N}-2}) \tag{5.2.12}$$

where $j'$ is a positive integer such that $j'/D(\Gamma) = j/D$ in the case when $D | D(\Gamma) j$. Note

that if $D \nmid D(\Gamma)j$, then $W_\Gamma(j) = 0$.

**A Brief Illustration of the above Estimate:**

To illustrate the above estimate, let us consider a simple example. Consider $p = 5, m = 4$ and $n = 1, r = 2$ so that $N = 2$ and assume that $\Sigma(\bar{f}, 2) = \Lambda(\bar{f}, 2)$, (cf. Remark 3.2.26), as as shown below. Thus, $\tilde{N} = N = 2$.

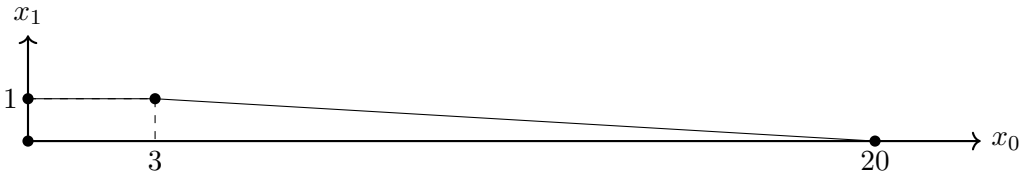



Figure 5.1: The level-2 $\Lambda$-diagram corresponding to $\bar{f}$ with $m = 4$ and $p = 5$

Let $\Gamma_1$ be the face defined by the hyperplane $w_1(x) = 1$ which is $x_1 = 1$ and let $\Gamma_2$ be the face defined by the hyperplane $w_2(x) = 1$ which is $x_0 + 17x_1 = 20$. Then $D(\Gamma_1) = 1, D(\Gamma_2) = 20$ and $D = 20$.

First consider $\Gamma_1$. For $0 < j$ with $20 \nmid j$, $D \nmid D(\Gamma_1)j$ and thus $W_{\Gamma_1}(j) = 0$, however, for $j = 20, 40, 60, ...$, we have that $j' = 1, 2, 3, ....$ For $j \geq 1$ for which $j' \equiv 0 \pmod 1$, $W_{\Gamma_1}(j)$ is a polynomial,

$$\begin{aligned} W_{\Gamma_1}(j) &= \frac{\tilde{V}(\Gamma_1)}{D(\Gamma_1)^{2-1}} j' + O(1) \\ &= 3j' + 1 \end{aligned}$$

in this case.

Now consider $\Gamma_2$. Now $D|D(\Gamma_2)j$ for all $j$ and $j' = j$ for all $j$. For each integer $s$ with $0 \leq s \leq 19$, consider all $j \geq 1$ for which $j' \equiv s \pmod{20}$. Then $W_{\Gamma_2}(j)$ is a polynomial,

$$\begin{aligned} W_{\Gamma_2}(j) &= \frac{\tilde{V}(\Gamma_2)}{D(\Gamma_2)^{2-1}} j' + O(1) \\ &= \left(\frac{1}{20}\right) j' + \frac{19s}{20} + 1 \end{aligned}$$

in this case.

---

Now, Equation 5.2.12 implies that for $x$ being an integer,

$$\sum_{j \leq Dx} W_\Gamma(j) = \sum_{j' \leq D(\Gamma)x} \frac{\tilde{V}(\Gamma)}{D(\Gamma)^{\tilde{N}-1}} (j')^{\tilde{N}-1} + O(x^{\tilde{N}-1}) \tag{5.2.13}$$

from which it is easily seen (please see Lemma 5.2.8) that

$$\sum_{j \leq Dx} W_\Gamma(j) = \frac{\tilde{V}(\Gamma)D(\Gamma)}{\tilde{N}} x^{\tilde{N}} + O(x^{\tilde{N}-1}) \tag{5.2.14}$$

**Lemma 5.2.8.** *Let $s$ be an integer, $x$ be a nonnegative real number and define $S_s(x)$ by* $\boxed{S_s(x) := \sum_{\substack{0 \leq y \leq x \\ y \in \mathbb{Z}}} y^s}$. *Then*

$$S_s(x) = \frac{x^{s+1}}{s+1} + O(x^s)$$

*Proof.* This is easily proven by using strong induction on $s$ as follows.

When $s = 1$, it is clear that $S_1(x) = \dfrac{x^2}{2} + O(x)$. Now, assume that $S_j(x) = \dfrac{x^{j+1}}{j+1} + O(x^j)$ for all $j = 1, 2, ..., k$. Now consider the following lemma.

**Lemma 5.2.9.** *Let $n = \lfloor x \rfloor$ and $k$ be an integer. Then, we have*

$$(x+1)^k - 1 = \sum_{s=0}^{k-1} \binom{k}{s} S_s(x) + O(x^{k-1}).$$

*Proof.*

$$\begin{aligned}
(x+1)^k - 1 &= (x+1)^k - 1^k \\
&= [(x+1)^k - (n+1)^k] + [(n+1)^k - n^k] + [n^k - (n-1)^k] + \ldots + [2^k - 1^k] \\
&= [(x+1)^k - (n+1)^k] + \sum_{m=1}^{n} [(m+1)^k - m^k]
\end{aligned}$$

$$
\begin{aligned}
&= [(x+1)^k - (n+1)^k] + \sum_{m=1}^{n} \sum_{i=1}^{k} \binom{k}{i} m^{k-i} \\
&= [(x+1)^k - (n+1)^k] + \sum_{i=1}^{k} \binom{k}{i} \sum_{m=1}^{n} m^{k-i} \\
&= [(x+1)^k - (n+1)^k] + \sum_{s=0}^{k-1} \binom{k}{s} \sum_{m=1}^{n} m^{s} \\
&= [(x+1)^k - (n+1)^k] + \sum_{s=0}^{k-1} \binom{k}{s} S_s(x) \\
&= \sum_{s=0}^{k-1} \binom{k}{s} S_s(x) + O(x^{k-1})
\end{aligned}
$$

where the last equality is due to the fact that

$$
\begin{aligned}
[(x+1)^k - (n+1)^k] &\leq [(n+2)^k - (n+1)^k] \\
&= O(n^{k-1}) \\
&= O(x^{k-1}).
\end{aligned}
$$

□

Then by the above lemma, we have

$$
(x+1)^{k+2} - 1 = \sum_{s=0}^{k+1} \binom{k+2}{s} S_s(x) + O(x^{k+1})
$$

from which we get

$$
\begin{aligned}
\binom{k+2}{k+1} S_{k+1}(x) &= [(x+1)^{k+2} - 1] - \sum_{s=0}^{k} \binom{k+2}{s} S_s(x) \\
\implies (k+2) S_{k+1}(x) &= x^{k+2} + O(x^{k+1})
\end{aligned}
$$

by the induction hypothesis, and whence we get

$$
S_{k+1}(x) = \frac{x^{k+2}}{(k+2)} + O(x^{k+1}).
$$

□

Now, by the definition of the volumes $\tilde{V}(\Gamma)$ and $\tilde{V}(\hat{\Gamma})$, it can be shown (please see Appendix D) that

$$\boxed{\frac{\tilde{V}(\Gamma)D(\Gamma)}{\tilde{N}} = \tilde{V}(\hat{\Gamma})}. \tag{5.2.15}$$

Then from equations 5.2.14 and 5.2.15, we get

$$\sum_{j \leq Dx} W_\Gamma(j) = \tilde{V}(\hat{\Gamma}) x^{\tilde{N}} + O(x^{\tilde{N}-1}). \tag{5.2.16}$$

And we can count $W(j)$ as follows. It is clear from equation 5.2.14 that

$$W(j) = \sum_{\Gamma}{}' W_\Gamma(j) - \sum_{\sigma}{}'' W_\sigma(j) + O(j^{\tilde{N}-2}) \tag{5.2.17}$$

where $\sum_{\Gamma}{}'$ denotes the sum over all $(\tilde{N}-1)$-dimensional faces $\Gamma$ of $\Sigma(\bar{f}, r)$ not containing the origin and $\sum_{\sigma}{}''$ denotes the sum over all $(\tilde{N}-2)$-dimensional faces $\sigma$ of $\Sigma(\bar{f}, r)$ that are the intersection of two $(\tilde{N}-1)$-dimensional faces occurring in $\sum_{\Gamma}{}'$.

Then, we can use equations to evaluate the term $\boxed{x \sum_{j \leq Dx} W(j)}$ as

$$x \sum_{j \leq Dx} W(j) = \sum_{\Gamma}{}' \tilde{V}(\hat{\Gamma}) x^{\tilde{N}+1} - \sum_{\sigma}{}'' \tilde{V}(\hat{\sigma}) x^{\tilde{N}} + O(x^{\tilde{N}-1}) \tag{5.2.18}$$

But since $\sum_{\Gamma}{}' \tilde{V}(\hat{\Gamma}) = \tilde{V}(\bar{f})$, we have from equation 5.2.18 that

$$\boxed{x \sum_{j \leq Dx} W(j) = \tilde{V}(\bar{f}) x^{\tilde{N}+1} + O(x^{\tilde{N}})}. \tag{5.2.19}$$

Now, we use a similar argument to deduce the other assertion of Theorem 5.2.6. Analogous to equation 5.2.12, we also have that

$$D^{-1} j W_\Gamma(j) = \frac{\tilde{V}(\Gamma)}{D(\Gamma)^{\tilde{N}}} (j')^{\tilde{N}} + O((j')^{\tilde{N}-1}) \tag{5.2.20}$$

from which we get, for $x$ being an integer,

$$D^{-1}\sum_{j\leq Dx} jW_\Gamma(j) = \sum_{j'\leq D(\Gamma)x} \frac{\tilde{V}(\Gamma)}{D(\Gamma)^{\tilde{N}}}(j')^{\tilde{N}} + O(x^{\tilde{N}}) \tag{5.2.21}$$

from which it is easily seen (again due to Lemma 5.2.8) that

$$D^{-1}\sum_{j\leq Dx} jW_\Gamma(j) = \frac{\tilde{V}(\Gamma)D(\Gamma)}{\tilde{N}+1}x^{\tilde{N}+1} + O(x^{\tilde{N}}). \tag{5.2.22}$$

Then from equation 5.2.15, we get

$$D^{-1}\sum_{j\leq Dx} jW_\Gamma(j) = \frac{\tilde{N}\tilde{V}(\hat{\Gamma})}{\tilde{N}+1}x^{\tilde{N}+1} + O(x^{\tilde{N}}). \tag{5.2.23}$$

Again since $\sum_{\Gamma}{}' \tilde{V}(\hat{\Gamma}) = \tilde{V}(\bar{f})$, using equation 5.2.17, we deduce that

$$\boxed{D^{-1}\sum_{j\leq Dx} jW(j) = \frac{\tilde{N}\tilde{V}(\bar{f})}{\tilde{N}+1}x^{\tilde{N}+1} + O(x^{\tilde{N}})} \tag{5.2.24}$$

thus proving Theorem 5.2.6.

# Chapter 6

# Conclusion and Future Directions

## 6.1 Conclusion

We summarize by quoting that in this thesis we considered the sequence of exponential sums,

$\left\{S_l^{A,r}(\Theta^{(r)}, \bar{f}) : l = 1, 2, ...\right\}$ where the $S_l^{A,r}(\Theta^{(r)}, \bar{f})$ are defined by

$$S_l^{A,r}(\Theta^{(r)}, \bar{f}) := \sum_{x \in \mathcal{T}_l^{A,r}} \Theta^{(r)} \circ \mathrm{Tr}_{R_l/R}(\bar{f}(\bar{x}))$$

where $r$ is an integer greater than or equal to 1, $\bar{f}(\bar{x})$ is a polynomial in $n$ variables, $\bar{x}_1, \bar{x}_2, ..., \bar{x}_n$ with coefficients in the Galois ring $R = \mathbb{Z}_q/p^r\mathbb{Z}_q$, $R_l \cong \mathbb{Z}_{q^l}/p^r\mathbb{Z}_{q^l}$ is the degree-$l$ Galois ring extension of $R$, $\mathrm{Tr}_{R_l/R}$ is the generalized trace map, $\Theta^{(r)}$ is a character of $\mathbb{Z}_p/p^r\mathbb{Z}_p$, $A = (A_1, A_2, ..., A_n)$ is an $n$-uple of subsets $A_i \subseteq \{0, 1, 2, ..., r-1\}$, $x = (x_1, x_2, ..., x_n)$ with the $x_i$ representing the level-$r$ $p$-adic expansion of the variable $\bar{x}_i$, that is, for each $i = 1, 2, ..., n$, we have

$$x_i = \sum_{j=0}^{r-1} x_{i,j} p^j$$

and the $x_{i,j}$ are called the *Teichmüller variables* associated to the variable, $\bar{x}_i$, and $\mathcal{T}_l^{A,r}$

is the set defined by

$$\mathcal{T}_l^{A,r} := \left\{ x = (x_1, x_2, ..., x_n) = \left( \sum_{j=0}^{r-1} x_{1,j} p^j, \ldots, \sum_{j=0}^{r-1} x_{n,j} p^j \right) \in R_l^n : \begin{cases} x_{i,j} \neq 0, & \text{if } j \in A_i \\ x_{i,j} = 0, & \text{if } j \notin A_i \end{cases} \right\}.$$

The associated $L$-function, $L^{A,r}(\Theta^{(r)}, \bar{f}, T)$ is defined by

$$L^{A,r}(\Theta^{(r)}, \bar{f}, T) := \exp\left( \sum_{l=1}^{\infty} \frac{S_l^{A,r}(\Theta^{(r)}, \bar{f}) T^l}{l} \right).$$

We studied the special case when $A = (J_r, J_r, ..., J_r)$ where $\boxed{J_r := \{0, 1, 2, ..., r-1\}}$ and we denoted the sequence of exponential sums by $S_l^*(\Theta^{(r)}, \bar{f})$ for $l = 1, 2, ...$ and the associated $L$-function by $L^*(\Theta^{(r)}, \bar{f}, T)$. In Chapter 3, we proved a generalized Dwork trace formula for this sequence of exponential sums by extending the work of Adolphhson and Sperber [AS87a] through construction of analogoues of Newton polyhedra associated to the polynomial $\bar{f}$. When $r = 1$, these exponential sums degenerate to the classical exponential sums over finite fields studied implicitly by Dwork [Dwo60] in his celebrated paper where he proves the rationality of the zeta function of an algebraic variety, and then later in more detail by Bombieri [Bom66], where he proves more results on the associated $L$-function.

The trace formula immediately gives us Dwork's classical results for the associated $L$-function $L^*(\Theta^{(r)}, \bar{f}, T)$. In particular, in Chapter 4, we deduced that this $L$-function is a finite alternating product of $p$-adically entire functions of $T$ which are Fredholm determinants of certain completely continuous operators called the *Dwork-Frobenius operators*. We then constructed the analogoue of the Dwork complex on which the Dwork-Forbenius operators act as a chain map, and thus realized the $L$-function in terms of Fredholm determinants of maps on the complex. This gives a corresponding statement on the cohomology of the complex as well.

In Chapter 5, we proved the rationality of the $L$-function using Dwork's classical methods. In that process, we generalized Bombieri's result ([Bom66]: Lemma 1) in Lemma 5.1.6 using the Galois theory of Galois rings. On obtaining generalized trace formulas for the sequence of exponential sums, $S_l^{A,r}(\Theta^{(r)}, \bar{f})$ for arbitrary $n$-uples $A =$

$(A_1, A_2, ..., A_n)$ of subsets of $J_r$, we can similarly prove the rationality of the associated $L$-function using Lemma 5.1.6 and its consequences. This leads us to a proof of rationality of the *zeta function*, $Z(V,T)$ of an affine variety, $V$ over the Galois ring, $R$ defined by

$$Z(V,T) := \exp\left(\sum_{l=1}^{\infty} \frac{N_l T^l}{l}\right) \tag{6.1.1}$$

where $N_l$ is the number of $R_l$-rational points of $V$ (please see section 5.1: Remark 5.1.15), by a simple combinatorial argument as in [Dwo60]. Meuser proved the rationality of this zeta function in [Meu86] as she studied a more general zeta function in two variables that generalized both the Weil zeta function and the Igusa zeta function. We have thus shown that there is an alternate proof for the rationality of the zeta function using Dwork's classical methods.

Later in Chapter 5, we proved the analogue of the Bombieri-Adolphson-Sperber estimate for the *degree* (the number of zeros minus the number of poles) of the associated $L$-function (or its reciprocal) in terms of the volume of the analogue of the *Newton polyhedron* [AS87a] of the polynomial, $\bar{f}$.

## 6.2 Future Directions

Here are a few applications and extensions of this work.

### 6.2.1 Rational Point Counts

An obvious application of this work is to obtain a formula for the number of $R_l$-rational points of an affine variety, $V$ over the Galois ring, $R$ in terms of the exponential sums of the kind $S_l^{A,r}(\Theta^{(r)}, \bar{f})$ by developing generalized Dwork trace formulas for arbitrary $n$-uples $A = (A_1, A_2, ..., A_n)$ of subsets $A_i \subseteq J_r$, and then by using the arguments in the end of section 1.5. We thus obtain results relating the zeta function 6.1.1 with the $L$-functions $L^{A,r}(\Theta^{(r)}, \bar{f}, T)$.

### 6.2.2 $p$-divisibility of the Number of Solutions

Another application of this work is to generalize Chevalley-Warning-Ax-Katz's classical result on the $p$-divisibility of the number of solutions to a system of polynomial equations defined over a finite field, to that corresponding to polynomial equations defined over Galois rings.

In 1935, Emil Artin conjectured that the finite field with $q$ elements, $\mathbb{F}_q$ is *quasi-algebraically closed*, that is, any homogeneous polynomial of degree, $d \neq 0$ in $n$ variables over $\mathbb{F}_q$ has a nontrivial zero provided $n > d$. His conjecture was motivated by the facts that both finite fields and quasi-algebraically closed fields have trivial Brauer groups (For proofs, please see [Ser79]: p.161-162). The Chevalley-Warning Theorem, first proven by Claude Chevalley [Che36] and then later strengthened and generalized by Ewald Warning [War36] implied immediately that Artin's conjecture was in fact true.

The Chevalley-Warning Theorem asserts that the cardinality of the set of common solutions in $\mathbb{F}_q^n$ to a system of $m$ polynomial equations in $n$ variables over $\mathbb{F}_q$ is divisible by the characteristic, $p$ of the field $\mathbb{F}_q$ as long as $n$ is greater than the sum of the total degrees of those polynomials. Later, James Ax [Ax64] strengthened the result by explicitly describing the power of $q$ dividing the cardinality to be at least

$$\left\lceil \frac{n - \sum_{i=1}^{m} d_i}{\sum_{i=1}^{m} d_i} \right\rceil$$

where $d_i$ is the total degree of the $i$-th polynomial and $\lceil x \rceil$ denotes the *ceiling function* of $x$, that is, $\lceil x \rceil$ is the smallest integer greater than or equal to $x$. In 1971, Nicholas Katz [Kat71] showed that this result could be strengthened further by asserting that the power of $q$ dividing the cardinality is at least

$$\left\lceil \frac{n - \sum_{i=1}^{m} d_i}{\max_i \{d_i\}} \right\rceil .$$

Marshall and Ramage [MR75] generalized Ax's results to the case of a single poly-

nomial defined over a finite principal ideal ring. More recently, Daniel J. Katz [Kat09] generalized Marshall-Ramage's [MR75] results and Nicholas Katz's [Kat71] results to the case of a system of polynomial equations over a finite principal ring. However, it is to be noted that Daniel J. Katz's generalization did not rely on Nicholas Katz's methods based on Dwork's $p$-adic theory. It would be interesting to obtain a generalization of Nicholas Katz's [Kat71] results for the case of a system of polynomial equations defined over Galois rings using the $p$-adic theory developed in this thesis by following Nicholas Katz's method, and compare the results with those obtained by Daniel J. Katz [Kat09].

On a related note, studying the $p$-divisibility of the exponential sums themselves has been of interest since the classical Stickelberger's congruence for Gauss sums. Adolphson and Sperber in [AS87b] investigated the $p$-divisibility of exponential sums over finite fields, and their result has been shown to imply Nicholas Katz's result [Kat71] on $p$-divisibility of the number of solutions. It is worth investigating a generalization of Adolphson-Sperber's results for our exponential sums over Galois rings.

### 6.2.3 Formalism in terms of an Artin $L$-function

The *Euler product* factorization for our $L$-functions that we deduced in Lemma 5.1.6 (that generalizes [Bom66]: Lemma 1) should, in principle, be derived based on a formalism in terms of certain Artin $L$-functions.

Bombieri [Bom66] relates the $L$-function, $L(f,T) = L(f,T,\mathbb{A}^n(\mathbb{F}_q))$ associated to sequence of *affine* exponential sums over finite fields,

$\{S_l(\Theta,f) = S_l(\Theta,f,\mathbb{A}^n(\mathbb{F}_q)) : l = 1,2,...\}$, where $\Theta$ is a nontrivial additive character of $\mathbb{F}_p$, $f$ is a polynomial over $\mathbb{F}_q$ and each of the sums

$$S_l(\Theta,f,,\mathbb{A}^n(\mathbb{F}_q) = \sum \Theta \circ \mathrm{Tr}_{\mathbb{F}_{q^l}/\mathbb{F}_p}(f(x))$$

is over all $x$ in $\mathbb{F}_{q^l}^n$; to the Artin $L$-function related to the Artin-Schreier covering (a Galois covering) of the affine $n$-space over the finite field $\mathbb{F}_q$ defined by the Artin-Schreier polynomial, $y^p - y = f(x)$ and the character $\Theta$ which is also a character of the Galois

group of the covering (which is isomorphic to $\mathbb{F}_p$). Realizing the $L$-function, $L(f,T)$ as such an Artin $L$-function immediately gave him the Euler product factorization. It is worthwhile to investigate the analogous formalism in terms of an Artin $L$-function for our $L$-function associated to exponential sums over Galois rings.

Such a formalism has been investigated by Liu and Wei [LW07]. They describe a Witt covering of $T^n$, the $n$-dimensional torus over $\mathbb{F}_q$ in terms of exponential sums over Galois rings. The case they examine is closely related to the sequence of exponential sums $\left\{S_l^{A,r} : l = 1, 2, ...\right\}$ where $A = (A_1, A_2, ..., A_n)$ with the $A_i = \{0\}$ for all $i$.

### 6.2.4 Twisted Exponential Sums generalizing Gauss Sums

We could extend this work by considering *twisted* exponential sums over Galois rings and generalize the work of Adolphson and Sperber [AS93].

On one hand, we could consider sums of the kind described as follows. We first observe that the group of all multiplicative characters $\chi : \mathbb{F}_p^\times \to \mathbb{C}_p^\times$ is generated by the *Teichmüller character*, $\omega : \mathbb{F}_p^\times \to \mathbb{C}_p^\times$ that sends an element $x$ in $\mathbb{F}_p^\times$ to its unique Teichmuller lift, $\omega(x) \in \mathbb{Z}_p$ which is a $(p-1)$-st root of unity. Hence any multiplicative character $\chi : \mathbb{F}_p^\times \to \mathbb{C}_p^\times$ is $\omega^k$ for some $k = 0, 1, 2, ..., p-2$. Now let $P = \mathbb{Z}_p/p^r\mathbb{Z}_p$, let $f$ be a polynomial in $n$ variables over the Galois ring $R = \mathbb{Z}_q/p^r\mathbb{Z}_q$, let $R_l$ be the degree-$l$ extension of $R$, let $\Theta$ be an additive character of $P$, and let $b = (b_{i,j})_{i=1,2,...,n;j=0,1,...,r-1}$ be a vector of $nr$ entries, each belonging to $\{0, 1, .., p-2\}$. Let $N_{R_l/P}$ and $\mathrm{Tr}_{R_l/P}$ denote the generalized norm and generalized trace maps respectively. Then the sequence of exponential sums, $\{S_l^{A,r}(b, \Theta, f) : l = 1, 2, ...\}$ with $A$ being the $n$-uple $A = (J_r, J_r, ..., J_r)$ where

$$S_l^{A,r}(b, \Theta, f) = \sum_{x \in \mathcal{T}_l^{A,r}} \left( \prod_{i=1}^{n} \prod_{j=0}^{r-1} \omega^{b_{i,j}} \circ N_{R_l/P}(x_{i,j}) \right) \Theta \circ \mathrm{Tr}_{R_l/P}(f(x))$$

where $\mathcal{T}_l^{A,r}$ is as defined earlier in this chapter, generalize the twisted exponential sums over finite fields considered by Adolphson and Sperber [AS93].

On the other hand, we could also consider a pair of characters $(\chi, \Theta)$ where $\Theta$ is

an additive character of $P := \mathbb{Z}_p/p^r\mathbb{Z}_p$, and $\chi$ is a multiplicative character of the group of units $P^*$ of $P$. Let $R$ be the Galois ring $\mathbb{Z}_q/p^r\mathbb{Z}_q$ and $R_l$ its degree-$l$ Galois ring extension for each $l$. Then the generalized norm maps $N_{R_l/P}$ and the generalized trace maps $\mathrm{Tr}_{R_l/P}$ give rise to a sequence of exponential sums, $\left\{S_l^{U,r}(\chi, \Theta, \bar{f}) : l = 1, 2, ...\right\}$ associated to a polynomial $\bar{f}$ (in several variables) over $R$, given by

$$S_l^{U,r}(\chi, \Theta, \bar{f}) = \sum \chi \circ N_{R_l/P}(\bar{x})\Theta \circ \mathrm{Tr}_{R_l/P}(\bar{f}(\bar{x}))$$

where the sum is over all $\bar{x} = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_n)$ with each $\bar{x}_i$ being a unit in the ring $R_l$. Note that the group of units of $R_l$ is a direct product $G_1 \times G_2$ where $G_1 = \mu_{q^l-1}$, the group of $(q^l - 1)$-th roots of unity and $G_2 = 1 + pR_l$ ([McD74], [Wan03]). The sum $S_l^{U,r}$ can easily be written in terms of the sums of the kind $S_l^{A,r}$ that we considered in this thesis.

These investigations would lead to extensions and variants of Xhumari's [Xhu16] and Blache's [Bla03] work on Gauss sums.

### 6.2.5 Finite Dimensionality of the Cohomology of the Dwork Complex

Another interesting question for future research is to find natural conditions for which the cohomology given in Chapter 4 is finite dimensional and computable. In the case when $r = 1$, conditions have been found where the cohomology vanishes except in the highest dimension and there it is finite dimensional. It would be of great interest to find such conditions in the case of sums over Galois rings.

# Bibliography


[Art59] Emil Artin, *Theory of Algebraic Numbers: Notes by Gerhard Würges from Lectures Held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester, 1956/7*, George Striker, 1959.

[AS87a] Alan Adolphson and Steven Sperber, *Newton Polyhedra and the degree of the L-function associated to an exponential sum*, Inventiones Mathematicae **Vol.88** (1987), 555–570.

[AS87b] ———, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning*, Annales scientifiques de l'É.N.S. 4 e série **20** (1987), 545–556.

[AS93] ———, *Twisted exponential sums and newton polyhedra*, Journal für die reine und angewandte Mathematik **443** (1993), 151–178.

[Ax64] James Ax, *Zeros of polynomials over finite fields*, American Journal of Mathematics **Vol.86** (1964), 255–261.

[Bla03] Régis Blache, *A Stickleberger Theorem for p-adic Gauss Sums*, Acta Arithmetica **118** (2003), 11–26.

[Bla09] ———, *L-functions of exponential sums on curves over rings*, Finite Fields and Their Applications, Elsevier **15 (3)** (2009), 345–359.

[Bom66] Enrico Bombieri, *On Exponential Sums in Finite Fields*, American Journal of Mathematics **Vol.88, No.1** (1966), 71–105.

[Bom78] ———, *On Exponential Sums in Finite Fields II*, Inventiones Mathematicae **47** (1978), 29–39.

[Che36] Claude Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg (in French) **Vol.11** (1936), 74–75.

[DL98] J. Denef and F. Loeser, *Motivic Igusa zeta Functions*, Journal of Algebraic Geometry **7** (1998), 505–537.

[Dwo60] Bernard Dwork, *On the Rationality of the Zeta Function of an Algebraic Variety*, American Journal of Mathematics **Vol.82** (1960), 631–648.

[Dwo62] ———, *On the zeta function of a hypersurface*, Publ. Math. I.H.E.S. **No.12** (1962), 5–68.

[Dwo64] ———, *On the zeta function of a hypersurface, II*, Annals of Mathematics **80** (1964), 227–299.

[Ehr67] Eugène Ehrhart, *Sur un problème de géométrie diophantienne linéare, I: Polyèdres et rèseaux*, J. Reine Angew. Math. **226** (1967), 1–29.

[Igu74] Jun-Ichi Igusa, *Complex powers and asymptotic expansions I. Functions of certain types*, Journal für die reine und angewandte Mathematik **268-269** (1974), 110–130.

[Kat71] Nicholas Katz, *On a Theorem of Ax*, American Journal of Mathematics **Vol.93, No. 2** (1971), 485–499.

[Kat09] Daniel J Katz, *Point Count Divisibility for Algebraic Sets over $\mathbb{Z}/p^\ell\mathbb{Z}$ and other Finite Principal Rings*, Proc. Amer. Math. Soc. **137** (2009), 4065–4075.

[KHC95] P. Vijay Kumar, Tor Helleseth, and A.R. Calderbank, *An Upper Bound for Weil Exponential Sums over Galois Rings and Applications*, IEEE Transactions on Information Theory **41** (1995), 456–468.

[Kob84] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta Functions*, 2nd ed., Springer-Verlag, 1984.

[Lan00] Serge Lang, *Algebraic Number Theory*, 2nd ed., Springer, 2000.

[Lan05] ———, *Algbra*, 3rd ed., Springer, 2005.

[LS00] P. Langevin and P. Solé, *Gauss Sums over quasi-Frobenius rings*, Proceedings of the fifth international conference on Finite Fields and Applications **Springer** (2000), 329–341.

[LW07] Chunlei Liu and Dasheng Wei, *The L-functions of Witt coverings*, Journal of Number Theory **255** (2007), 95–115.

[LW09] Chunlei Liu and Daqing Wan, *T-adic Exponential Sums over Finite Fields*, Algebra and Number Theory **3, 5** (2009), 489–509.

[Mat89] Hideyuki Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1989.

[McD74] B.R. McDonald, *Finite Rings with Identity*, New York: Marcel Dekker, 1974.

[Meu86] Diane Meuser, *The Meromorphic Continuation of a Zeta Function of Weil and Igusa type*, Inventiones Mathematicae **85** (1986), 493–514.

[Mon70] Paul Monsky, *p-adic Analysis and Zeta Functions*, Kinokuniya Book-Store Co., Ltd., 1970.

[MR75] Murray Marshall and Garry Ramage, *Zeros of polynomials over finite principal ideal rings*, Proc. Amer. Math. Soc. **49** (1975), 35–38.

[Mus11] Mircea Mustata, *Zeta Functions in Algebraic Geometry - Lecture Notes*, `http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf`, 2011.

[PGS10] C. Perez-Garcia and W.H. Schikhof, *Locally Convex Spaces over Non-Archimedian Valued Fields*, Cambridge University Press, 2010.

[Rab14] Joseph Rabinoff, *The Theory of Witt Vectors*, `https://arxiv.org/pdf/1409.7445.pdf`, 2014.

[Ser62] Jean-Pierre Serre, *Endomorphismes complètement continus des espaces de Banach p-adiques*, Publications mathématiques de l'I.H.É.S. **Vol.12, No.2** (1962), 69–85.

[Ser79] ———, *Local Fields*, Springer-Verlag, 1979.

[Sil09] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, 2009.

[Wan03] Zhe-Xian Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing, 2003.

[War36] Ewald Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg (in German) **Vol.82** (1936), 76–83.

[Wei49] André Weil, *Number of Solutions of Equations in Finite Fields*, Bulletin of American Mathematical Society **Vol.55, No. 5** (1949), 453–544.

[Wit36] Ernst Witt, *"Zyklische Körper und Algebren der Characteristik p vom Grad $p^n$. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik $p^n$"*, Journal für die Reine und Angewandte Mathematik (in German) **176** (1936), 126–140.

[Xhu16] Sandi Xhumari, *Generalized p-adic gauss sums*, Ph.D. thesis, University of Connecticut - Storrs, 2016.

# Appendices

# Appendix A

# Hilbert's Theorem 90 for Galois Rings

We will state and prove the analogue of Hilbert's Theorem 90 (Additive Form) for Galois rings. This is an exercise in [Wan03].

**Proposition A.0.1.** *Let $p$ be a prime, let $a$ be a positive integer, and let $q = p^a$. Let $R$ denote the Galois ring $GR(p^r, a)$ that has characteristic $p^r$ and cardinality, $q^r$. Let $R_l$ be the degree-$l$ Galois ring extension of $R$. (So $R_l$ is isomorphic to $GR(p^r, al)$ and it contains $R$ as a subring). Let $\sigma$ be the generalized Frobenius generator of the Galois group, $Gal(R_l/R)$, and let $\mathrm{Tr}_{R_l/R}$ denote the generalized trace map. Then we have:*

*(i) For $b \in R_l$, $\mathrm{Tr}(b) = 0$ if and only if there is some $a \in R_l$ such that $b = a - \sigma(a)$.*

*(ii) The generalized trace map $\mathrm{Tr}_{R_l/R} : R_l \to R$ is surjective.*

*Proof.*

(i) If $b = a - \sigma(a)$ for some $a \in R_l$, then it is clear that $\mathrm{Tr}_{R_l/R}(b) = a - \sigma^l(a) = 0$.

Conversely, suppose that $\mathrm{Tr}_{R_l/R}(b) = 0$. Let $F$ and $F_l$ denote the residue fields of $R$ and $R_l$ respectively. Let $\bar{\sigma}$ denote the Frobenius generator of the Galois group,

$Gal(F_l/F)$. Since the trace map, $\mathrm{Tr}_{F_k/F} : F_k \to F$ is nonzero, there is some $\bar{c} \in F_k$ such that $\mathrm{Tr}_{F_k/F}(\bar{c}) \neq 0$. Then, the Teichmüller lift, $c \in \mathbb{Z}_{q^l}$ of $\bar{c}$ reduces to $\bar{c}$ (mod $p$) and it is a unit in $R_l$ such that $\mathrm{Tr}_{R_l/R}(c) \neq 0$. Let $t = \mathrm{Tr}_{R_l/R}(c)$. Then, it is clear that $t$ is a unit in $R$.

Now, we may imitate Hilbert's classical argument in this setting. Let $a \in R_l$ be the element defined by

$$a := \frac{1}{t}\Big(bc + [b+\sigma(b)]\sigma(c) + [b+\sigma(b)+\sigma^2(b)]\sigma^2(c) + \ldots \\ +[b+\sigma(b)+\ldots+\sigma^{l-1}(b)]\sigma^{l-1}(c)\Big).$$

Then since $\mathrm{Tr}_{R_l/R}(b) = 0$,

$$a - \sigma(a) = \frac{1}{t}\left[b\sum_{i=0}^{l-1}\sigma^i(c) - \sigma^l(c)\sum_{i=1}^{l}\sigma^i(b)\right] = \frac{1}{t}[bt - c\cdot 0] = b.$$

(ii) The trace map, $\mathrm{Tr}_{R_l/R} : R_l \to R$ is an $R$-module homomorphism. Let $K$ be the kernel of this map. Then by (i), we have that

$$K = \{a - \sigma(a) : a \in R_l\}.$$

Then clearly, $a - \sigma(a) = a' - \sigma(a')$ if and only if $a - a' = \sigma(a - a')$ if and only if $(a - a') \in R$ if and only if $a$ and $a'$ are in the same coset in relative to $R$ in the additive abelian group $R_l$. Hence, the cardinality, $|K|$ of $K$ is the index, $[R_l : R]$ of the subgroup $R$ of $R_l$.

Then it is clear that the cardinality of the image $\mathrm{Im}(\mathrm{Tr}_{R_l/R})$ is given by

$$|\mathrm{Im}(\mathrm{Tr}_{R_l/R})| = \frac{|R_l|}{|K|} = \frac{|R_l|}{[R_l : R]} = |R|.$$

Thus the trace map $\mathrm{Tr}_{R_l/R}$ is surjective.

□

# Appendix B

# Proofs of Some Basic Facts given in Chapter 2

## B.1 Proof of Proposition 2.1.8

*Proof.* Let us first show the existence. If $\alpha = 0$, then we just take $\tilde{\alpha} = 0$. Now suppose $\alpha \neq 0$. By the previous proposition 2.1.7, $\mathbb{Q}_{p^f} = \mathbb{Q}_p(\tilde{\beta})$ where $\tilde{\beta} \in \bar{\mathbb{Q}}_p$ is a primitive $(p^f - 1)$-th root of unity and its image $\beta \in \mathbb{Z}_{p^f}/p\mathbb{Z}_{p^f} \cong \mathbb{F}_{p^f}$ is also a primitive $(p^f - 1)$-th root of unity. Hence $\beta$ is a generator of $\mathbb{F}_{p^f}^{\times}$ and thus $\alpha = \beta^k$ for some integer $k$. Since $\tilde{\beta} \in \mathbb{Z}_{p^f}$, we may take $\tilde{\alpha} = \tilde{\beta}^k \in \mathbb{Z}_{p^f}$. Then $\tilde{\alpha}$ has the required properties.

We will now show the uniqueness. It follows easily from Hensel's Lemma [Mat89]. Suppose $\tilde{\alpha}, \tilde{\beta} \in \mathbb{Z}_{p^f}$ are two different lifts of $\alpha$ satisfying $\tilde{\alpha}^{p^f} = \tilde{\alpha}$ and $\tilde{\beta}^{p^f} = \tilde{\beta}$. The monic polynomial $(x^{p^f-1} - 1)$ over $\mathbb{Z}_{p^f}$ reduces to itself $\pmod{p\mathbb{Z}_{p^f}}$ and is separable over $\mathbb{F}_{p^f}$ and factors into $p^f - 1$ distinct linear factors $(x - \alpha_i)$, with the $\alpha_i$ being the nonzero elements of $\mathbb{F}_{p^f}$. Then since the factors $(x-\alpha)$ and $(x^{p^f-1}-1)/(x-\alpha)$ are relatively prime monic polynomials, by Hensel's Lemma, there exists $\alpha' \in \mathbb{Z}_{p^f}$ and a monic polynomial $G(x) \in \mathbb{Z}_{p^f}[x]$ such that $(x^{p^f-1} - 1) = (x - \alpha')G(x)$ such that $\alpha'$ reduces to $\alpha$ and $G(x)$ reduces to $(x^{p^f-1} - 1)/(x - \alpha) \pmod{p\mathbb{Z}_{p^f}}$. Repeating the argument for the monic polynomial $G(x)$, we see that the polynomial $(x^{p^f-1} - 1)$ is separable over

$\mathbb{Q}_{p^f}$ and

$$x^{p^f-1} - 1 = \prod_{i=1}^{p^f-1} (x - \alpha_i')$$

where the $\alpha_i' \in \mathbb{Z}_{p^f}$ reduce to $\alpha_i \in \mathbb{F}_{p^f}$ which are all distinct. Hence if both $\tilde{\alpha}$ and $\tilde{\beta}$ reduce to the same $\alpha$, they must coincide. □

## B.2 Proof of Corollary 2.1.10

*Proof.* We first consider the special case when $\alpha \in \mathbb{Z}_{p^f}$. Let $a_0$ be the Teichmüller lift of the image of $\alpha$ in $\mathbb{F}_{p^f}$. Then $\alpha - a_0 = p\alpha_1$ for some $\alpha_1 \in \mathbb{Z}_{p^f}$. Repeat this construction for $\alpha_1$ to get $\alpha_1 - a_1 = p\alpha_2$ for some $\alpha_2 \in \mathbb{Z}_{p^f}$ where $a_1$ is the Teichmüller lift of the image of $\alpha_1$ in $\mathbb{F}_{p^f}$. In this way, we have the existence of such a series representation:

$$\alpha = \sum_{i=0}^{\infty} a_i p^i$$

with the $a_i$ satisfying $a_i^{p^f} = a_i$ for all $i \geq 0$. The uniqueness of this expression follows from the uniqueness of the Teichmüller lifts as per the previous proposition. For example, if $\alpha = \sum_{i\geq 0} a_i p^i = \sum_{i\geq 0} b_i p^i$, with $a_i^{p^f} = a_i$ and $b_i^{p^f} = b_i$, then by considering the reduction modulo $p\mathbb{Z}_{p^f}$, we easily see successively that $a_i = b_i$ for every $i$.

Now for the general case when $\alpha \in K$ as in the second part of the statement of the corollory, we first observe that $\alpha$ can be written uniquely of the form $\alpha = \pi^m u$ for some unit $u \in \mathcal{O}_K$, where $\mathcal{O}_K = \{x \in K : \operatorname{ord}_p x \geq 0\}$ is the ring of integers of $K$, with $\operatorname{ord}_p u = 0$ and $m$ being the integer such that $m = e \operatorname{ord}_p \alpha$. We also note that $K = \mathbb{Q}_{p^f}(\pi)$ by proposition 2.1.7. Now we imitate the same construction as in the previous paragraph by considering the reduction of $u$ modulo $\pi\mathcal{O}_K$ in $\mathbb{F}_{p^f}$ and lifting it back to its unique Teichmüller lift to obtain the expression,

$$u = \sum_{i=0}^{\infty} b_i \pi^i.$$

The uniqueness of this expression follows from the uniqueness of the Teichmüller units $b_i$ in the same way as before. Then by multiplying by $\pi^m$, we obtain the expression

$$\alpha = \sum_{i=m}^{\infty} a_i \pi^i$$

where $a_i = b_{i-m}$ satisfy $a_i^{p^f} = a_i$ for every $i \geq m$.

□

## B.3 Proof of Proposition 2.1.11

*Proof.* Firstly, if $\sigma$ is an embedding of $\mathbb{Q}_{p^f}$ into an algebraic closure $\bar{\mathbb{Q}}_p$, then we observe that $\sigma(\mathbb{Q}_{p^f})$ is an unramified extension of $\mathbb{Q}_p$ of degree $f$. This is because of the fact [Art59] that any valuation of rank 1 of a complete field can be extended uniquely to a finite extension, and in particular, the extension can precisely be given in a formula using the absolute values of elements of the base field. In our case, the valuation on $\mathbb{Q}_{p^f}$ extending the $p$-adic valuation on $\mathbb{Q}_p$ is precisely given by $|\alpha| = \left|N_{\mathbb{Q}_{p^f}/\mathbb{Q}_p}(\alpha)\right|_p^{(1/f)}$ for any $\alpha \in \mathbb{Q}_{p^f}$. In particular, this implies that $|\sigma(\alpha)| = |\alpha|$, or in other words, $\mathrm{ord}_p\, \sigma(\alpha) = \mathrm{ord}_p\, \alpha$ for every $\alpha \in \mathbb{Q}_{p^f}$. Hence, the extension $\sigma(\mathbb{Q}_{p^f})$ over $\mathbb{Q}_p$ is unramified as well. Then, by the uniqueness of the unramified extension (Proposition 2.1.7), it follows that $\sigma(\mathbb{Q}_{p^f}) = \mathbb{Q}_{p^f}$. Also evidently the extension $\mathbb{Q}_{p^f}$ is separable over $\mathbb{Q}_p$ which has characteristic zero. Hence, $\mathbb{Q}_{p^f}$ is Galois over $\mathbb{Q}_p$.

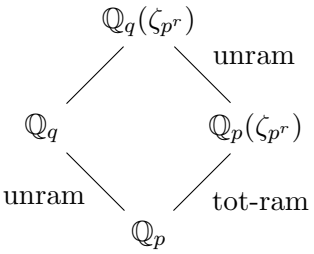
Now, any automorphism $\sigma$ of $\mathbb{Q}_{p^f}$ fixing $\mathbb{Q}_p$ induces an automorphism of $\mathbb{Z}_{p^f}$, which in turn induces an automorphism, $\overline{\sigma}$ of the residue class field $\mathbb{Z}_{p^f}/p\mathbb{Z}_{p^f} \cong \mathbb{F}_{p^f}$. Hence we have a group homomorphism, $g : Gal(\mathbb{Q}_{p^f}/\mathbb{Q}_p) \to Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$ of finite groups of the same order equalling $f$. Now, $\mathbb{Q}_{p^f} = \mathbb{Q}_p(\tilde{\alpha})$ for some primitive $(p^f - 1)$-th root of 1, $\tilde{\alpha} \in \overline{\mathbb{Q}}_p$. Also the image $\alpha$ of $\tilde{\alpha}$ in the residue class field $\mathbb{Z}_{p^f}/p\mathbb{Z}_{p^f}$ is also a primitive $(p^f - 1)$-th root of 1. Hence, for any $\sigma \in Gal(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$, the conjugate $\sigma(\tilde{\alpha}) = \tilde{\alpha}^i$ for some integer $i$, and hence it can easily be seen that $g$ is injective, and hence an isomorphism. □

## B.4 Proof of Lemma 2.1.12

*Proof.* For $(i)$, since $\overline{\sigma}(\bar{x}) = \bar{x}^p = \overline{x^p}$, we have that $\overline{\sigma(x)} = \overline{x^p}$ and thus $\sigma(x) \equiv x^p \pmod{p\mathbb{Z}_{p^f}}$. For $(ii)$, first it is easy to observe that if $x$ is a Teichmüller lift, then so is $\sigma(x)$ because $\sigma(x)^{p^f} = \sigma(x^{p^f}) = \sigma(x)$. By $(i)$, $\sigma(x)$ must satisfy $\sigma(x) \equiv x^p \pmod{p\mathbb{Z}_{p^f}}$. But then $x^p$ is a Teichmüller lift satisfying $x^p \equiv x^p \pmod{p\mathbb{Z}_{p^f}}$. By the uniquenuess of Teichmüller lifts, we must have that $\sigma(x) = x^p$. □

## B.5 Proof of Proposition 2.1.23

*Proof.* We have the following tower of fields.




We will first establish that the degree $[\mathbb{Q}_q(\zeta_{p^r}) : \mathbb{Q}_p(\zeta_{p^r})] = [\mathbb{Q}_q : \mathbb{Q}_p] = a$. Since $\mathbb{Q}_q$ is unramified over $\mathbb{Q}_p$ and since $\mathbb{Q}_p(\zeta_{p^r})$ is finite over $\mathbb{Q}_p$, we have that the compositum $\mathbb{Q}_q(\zeta_{p^r})$ is unramified over $\mathbb{Q}_p(\zeta_{p^r})$ by [Lan00] (Chapter II: Section 4 - Proposition 8) and thus the degree, $[\mathbb{Q}_q(\zeta_{p^r}) : \mathbb{Q}_p(\zeta_{p^r})]$ equals the residue field degree, $f_{\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})}$. Now, on one hand, the residue field degree, $f$ of the extension $\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p$ being the product of the residue field degrees of the extensions $\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})$ and $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$, must coincide with the residue field degree of the extension $\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})$ as the latter extension is totally ramifed (It can be shown that $(\zeta_{p^r} - 1)$ is a root of an *Eisenstein* polynomial of degree $p^{r-1}(p-1)$). On the other hand, we have $f \geq f_{\mathbb{Q}_q/\mathbb{Q}_p} = a$, the residue field degree of $\mathbb{Q}_q/\mathbb{Q}_p$. Hence we have that

$$[\mathbb{Q}_q(\zeta_{p^r}) : \mathbb{Q}_p(\zeta_{p^r})] = f_{\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})} = f \geq a.$$

However, since $\mathbb{Q}_q(\zeta_{p^r}) = \mathbb{Q}_p(\zeta_{p^r}, \zeta_{p^a-1})$, and since $\zeta_{p^a-1}$ satisfies a polynomial of degree

$a$ over $\mathbb{Q}_p(\zeta_{p^r})$, we have that the degree

$$[\mathbb{Q}_q(\zeta_{p^r}) : \mathbb{Q}_p(\zeta_{p^r})] \leq a.$$

Therefore,

$$[\mathbb{Q}_q(\zeta_{p^r}) : \mathbb{Q}_p(\zeta_{p^r})] = a.$$

Now, if $\tau : \mathbb{Q}_q(\zeta_{p^r}) \hookrightarrow \overline{\mathbb{Q}}_p$ is any embedding fixing $\mathbb{Q}_p(\zeta_{p^r})$, then since $\tau$ fixes $\mathbb{Q}_p$, its restriction, $\tau|_{\mathbb{Q}_q} \in Gal(\mathbb{Q}_q/\mathbb{Q}_p)$ and thus $\tau(\mathbb{Q}_q) = \mathbb{Q}_q$. Also since $\tau$ fixes $\zeta_{p^r}$, we have that $\tau(\mathbb{Q}_q(\zeta_{p^r})) = \mathbb{Q}_q(\zeta_{p^r})$. So the extension $\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})$ is normal, and since $\mathbb{Q}_p(\zeta_{p^r})$ has characteristic zero, it follows that the extionsion is Galois.

Finally, consider the map $\psi : Gal(\mathbb{Q}_q(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^r})) \longrightarrow Gal(\mathbb{Q}_q/\mathbb{Q}_p)$ defined by $\psi : \tau \mapsto \tau|_{\mathbb{Q}_q}$. Since $\tau(\zeta_{p^r}) = \zeta_{p^r}$, this map is clearly an injective homomorphism of finite groups of the same order, and is hence an isomorphism. □

## B.6 Proof of Lemma 2.2.3

*Proof.* Suppose that $T$ is affinely independent. Consider the linear equation

$$c_2(v_2 - v_1) + c_3(v_3 - v_1) + \ldots + c_k(v_k - v_1) = 0$$

which can be rewritten as

$$c_2v_2 + c_3v_3 + \ldots c_kv_k - (c_2 + c_3 + \ldots + c_k)v_1 = 0.$$

It is clear that the scalars $c_i$ must equal 0 for all $i = 2, 3, ..., k$ for otherwise the above equation violates the assumption that $T$ is affinely independent as we note that

$$c_2 + c_3 + \ldots c_k - (c_2 + c_3 + \ldots + c_k) = 0.$$

Conversely suppose $S$ is linearly independent. Consider the linear equation

$$d_1v_1 + d_2v_2 + \ldots + d_kv_k = 0$$

where the scalars $d_1, d_2, ..., d_k$ satisfy $\sum_{i=1}^{k} d_i = 0$. Then we may write $d_1 = -(d_2 + d_3 + \ldots + d_k)$, from which the above equation becomes

$$-(d_2 + d_3 + \ldots + d_k)v_1 + d_2v_2 + \ldots + d_kv_k = 0$$

which can be rewritten as

$$d_2(v_2 - v_1) + d_3(v_3 - v_1) + \ldots + d_k(v_k - v_1) = 0.$$

Then from the linear independence of $S$, it follows that $d_i = 0$ for $i = 2, 3, ..., k$, whence

$$d_1 = -(d_2 + d_3 + \ldots + d_k) = 0.$$

□

# Appendix C

# Proof of Proposition 3.1.29 in Chapter 3

In this appendix, we will prove Proposition 3.1.29. The proof, although tedious, is very analogous to the proof of Proposition 3.1.19. Let us rewrite equations 3.1.13, 3.1.14 and 3.1.15 below so that it is easier follow the proof.

$$
\begin{aligned}
&[h_{(0,1,1)} + 2h_{(0,2,1)} + 3h_{(0,3,1)} + \ldots + mh_{(0,m,1)}] \\
&+[0 + h_{(0,2,2)} + 2h_{(0,3,2)} + \ldots + (m-1)h_{(0,m,2)}] \\
&+[0 + h_{(0,2,3)} + 2h_{(0,3,3)} + \ldots + (m-1)h_{(0,m,3)}] \\
&+[0 + 0 + h_{(0,2,4)} + \ldots + (m-2)h_{(0,m,4)}] \\
&+[h_{(1,1,1)} + 2h_{(1,2,1)} + 3h_{(1,3,1)} + \ldots + mh_{(1,m,1)}] \\
&+[0 + h_{(1,1,2)} + 2h_{(1,2,2)} + \ldots + (m-1)h_{(1,m,2)}] \\
&+[h_{(2,1,1)} + 2h_{(2,2,1)} + 3h_{(2,3,1)} + \ldots + mh_{(2,m,1)}] = \kappa_0 \qquad \text{(C.0.1)} \\
&[h_{(0,1,2)} + h_{(0,2,2)} + \ldots + h_{(0,m,2)}] \\
&+[0 + 2h_{(0,2,4)} + \ldots + 2h_{(0,m,4)}] \\
&+[h_{(1,1,2)} + h_{(1,2,2)} + \ldots + h_{(1,m,2)}] = \kappa_1 \qquad \text{(C.0.2)} \\
&h_{(0,1,3)} + h_{(0,2,3)} + \ldots + h_{(0,m,3)} = \kappa_2 \qquad \text{(C.0.3)}
\end{aligned}
$$

**Proposition C.0.1** (Proposition 3.1.29)**.** *For $\kappa = (\kappa_0, \kappa_1, \kappa_2) \in \mathbb{Z}^3_{\geq 0}$, one has*

$$p^2 w(\kappa) \geq w_\Delta(\kappa)$$

*Proof.* We have

$$\begin{aligned}
w(\kappa) &= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, r, \kappa)} \left\{ \sum_{s=0}^{r-1} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,r)} \left( \frac{1}{p^{r-1}} \right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\} \\
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, 3, \kappa)} \left\{ \sum_{s=0}^{2} \sum_{\mu=1}^{m} \sum_{i_{(s,\mu)}=1}^{\bar{\rho}(s,\mu,3)} \left( \frac{1}{p} \right) \cdot p^{d(k^{(s,\mu,i_{(s,\mu)})})+s} \cdot h_{(s,\mu,i_{(s,\mu)})} \right\} \\
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, 3, \kappa)} \left\{ \left( \frac{1}{p^2} \right) \sum_{\mu=1}^{m} h_{(0,\mu,1)} + \left( \frac{1}{p} \right) \left[ \sum_{\mu=1}^{m} h_{(0,\mu,2)} + \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right] \right. \\
&\qquad \left. + \left[ \sum_{\mu=1}^{m} h_{(0,\mu,3)} + \sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)} + \sum_{\mu=1}^{m} h_{(2,\mu,1)} \right] \right\} \\
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f}, 3, \kappa)} \left\{ \left( \frac{1}{p^2} \right) \sum_{\mu=1}^{m} h_{(0,\mu,1)} + \left( \frac{1}{p} \right) \left[ \sum_{\mu=1}^{m} h_{(0,\mu,2)} + \sum_{\mu=1}^{m} h_{(1,\mu,1)} \right] \right. \\
&\qquad \left. + \left[ \kappa_2 + \sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)} + \sum_{\mu=1}^{m} h_{(2,\mu,1)} \right] \right\}
\end{aligned} \tag{C.0.4}$$

where the last equality follows from Equation C.0.3.

Now if $h \in J_{\mathbb{Q}}(\bar{f}, 3, \kappa)$, then since all of its components are nonnegative, we have from Equation C.0.1 that

$$\begin{aligned}
&m[h_{(0,1,1)} + h_{(0,2,1)} + h_{(0,3,1)} + \ldots + h_{(0,m,1)}] \\
+&(m-1)[h_{(0,1,2)} + h_{(0,2,2)} + h_{(0,3,2)} + \ldots + h_{(0,m,2)}] \\
+&(m-1)[h_{(0,1,3)} + h_{(0,2,3)} + h_{(0,3,3)} + \ldots + h_{(0,m,3)}] \\
+&2(m-1)[h_{(0,2,4)} + h_{(0,3,4)} + \ldots + h_{(0,m,4)}] \\
+&m[h_{(1,1,1)} + h_{(1,2,1)} + h_{(1,3,1)} + \ldots + h_{(1,m,1)}] \\
+&(m-1)[h_{(1,1,2)} + h_{(1,2,2)} + h_{(1,3,2)} + \ldots + h_{(1,m,2)}] \\
+&m[h_{(2,1,1)} + h_{(2,2,1)} + h_{(2,3,1)} + \ldots + h_{(2,m,1)}] \geq \kappa_0.
\end{aligned}$$

Then by using equations C.0.2 and C.0.3 in the above inequality, we arrive at

$$\sum_{\mu=1}^{m} h_{(0,\mu,1)} \geq \left(\frac{1}{m}\right)\kappa_0 - \left(\frac{m-1}{m}\right)\kappa_1 - \left(\frac{m-1}{m}\right)\kappa_2 - \sum_{\mu=1}^{m} h_{(1,\mu,1)} - \sum_{\mu=1}^{m} h_{(2,\mu,1)}.$$

Using the above inequality in Equation C.0.4, we have

$$w(\kappa) \geq \inf_{h\in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \left\{ \left(\frac{1}{p^2}\right)\left[\left(\frac{\kappa_0}{m}\right) - \left(\frac{m-1}{m}\right)(\kappa_1+\kappa_2) - \sum_{\mu=1}^{m} h_{(1,\mu,1)} - \sum_{\mu=1}^{m} h_{(2,\mu,1)}\right] + \left(\frac{1}{p}\right)\left[\sum_{\mu=1}^{m} h_{(0,\mu,2)} + \sum_{\mu=1}^{m} h_{(1,\mu,1)}\right] + \left[\kappa_2 + \sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)} + \sum_{\mu=1}^{m} h_{(2,\mu,1)}\right]\right\}$$

Hence, we have

$$\begin{aligned} p^2 w(\kappa) &\geq \inf_{h\in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \left\{ \left[\left(\frac{\kappa_0}{m}\right) - \left(\frac{m-1}{m}\right)(\kappa_1+\kappa_2) \right.\right. \\ &\qquad \left. + (p-1)\sum_{\mu=1}^{m} h_{(1,\mu,1)} + (p^2-1)\sum_{\mu=1}^{m} h_{(2,\mu,1)}\right] \\ &\qquad + p\sum_{\mu=1}^{m} h_{(0,\mu,2)} \\ &\qquad \left. + p^2\left[\kappa_2 + \sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)}\right]\right\} \\ &= \inf_{h\in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \left\{ \left[\left(\frac{\kappa_0}{m}\right) - \left(\frac{m-1}{m}\right)(\kappa_1+\kappa_2) \right.\right. \\ &\qquad \left. + (p-1)\sum_{\mu=1}^{m} h_{(1,\mu,1)} + (p^2-1)\sum_{\mu=1}^{m} h_{(2,\mu,1)}\right] \\ &\qquad + p\left[\sum_{\mu=1}^{m} h_{(0,\mu,2)} + 2\sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)}\right] \\ &\qquad \left. + p^2\kappa_2 + \left[(p^2-2p)\sum_{\mu=2}^{m} h_{(0,\mu,4)} + (p^2-p)\sum_{\mu=1}^{m} h_{(1,\mu,2)}\right]\right\} \end{aligned}$$

$$
\begin{aligned}
&= \inf_{h \in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \Bigg\{ \Bigg[ \left(\frac{\kappa_0}{m}\right) - \left(\frac{m-1}{m}\right)(\kappa_1+\kappa_2) \\
&\qquad\qquad + (p-1)\sum_{\mu=1}^{m} h_{(1,\mu,1)} + (p^2-1)\sum_{\mu=1}^{m} h_{(2,\mu,1)} \Bigg] \\
&\qquad\qquad + p\kappa_1 \\
&\qquad\qquad + p^2\kappa_2 + \left[ (p^2-2p)\sum_{\mu=2}^{m} h_{(0,\mu,4)} + (p^2-p)\sum_{\mu=1}^{m} h_{(1,\mu,2)} \right] \Bigg\} \\
&\geq \left(\frac{1}{m}\right)\kappa_0 - \left[p - \left(\frac{m-1}{m}\right)\right]\kappa_1 + \left[p^2 - \left(\frac{m-1}{m}\right)\right]\kappa_2 \\
&= w_2(\kappa).
\end{aligned}
$$

On the other hand, from Equation C.0.4, we also have

$$
\begin{aligned}
w(\kappa) &= \inf_{h \in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \Bigg\{ \left(\frac{1}{p^2}\right)\sum_{\mu=1}^{m} h_{(0,\mu,1)} + \left(\frac{1}{p}\right)\left[\sum_{\mu=1}^{m} h_{(0,\mu,2)} + \sum_{\mu=1}^{m} h_{(1,\mu,1)}\right] \\
&\qquad\qquad + \left[\kappa_2 + \sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)} + \sum_{\mu=1}^{m} h_{(2,\mu,1)}\right] \Bigg\} \\
\implies p^2 w(\kappa) &= \inf_{h \in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \Bigg\{ \sum_{\mu=1}^{m} h_{(0,\mu,1)} + p\left[\sum_{\mu=1}^{m} h_{(0,\mu,2)} + \sum_{\mu=1}^{m} h_{(1,\mu,1)}\right] \\
&\qquad\qquad + p^2\left[\kappa_2 + \sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)} + \sum_{\mu=1}^{m} h_{(2,\mu,1)}\right] \Bigg\} \\
&\geq \inf_{h \in J_{\mathbb{Q}}(\bar{f},3,\kappa)} \Bigg\{ 0 + p\left[\sum_{\mu=1}^{m} h_{(0,\mu,2)} + 2\sum_{\mu=2}^{m} h_{(0,\mu,4)} + \sum_{\mu=1}^{m} h_{(1,\mu,2)} + 0\right] \\
&\qquad\qquad + p^2\kappa_2 + (p^2-2p)\sum_{\mu=2}^{m} h_{(0,\mu,4)} + (p^2-p)\sum_{\mu=1}^{m} h_{(1,\mu,2)} + 0 \Bigg\} \\
&\geq p\kappa_1 + p^2\kappa_2 = w_1(\kappa)
\end{aligned}
$$

where the last inequality follows from Equation C.0.2 and from the fact that the $h_{(s,\mu,i_{(s,\mu)})}$ are all nonnegative.

And thus, we have

$$p^2 w(\kappa) \geq \max\{w_1(\kappa), w_2(\kappa)\} = w_\Delta(\kappa).$$

□

# Appendix D

# Proof of Equation 5.2.15 in Chapter 5

In this appendix, we will prove Equation 5.2.15 in Chapter 5.

**Proposition D.0.1.** *Let $\tilde{N}$ be the dimension of $E(\bar{f})$, the smallest subspace of $\mathbb{R}^N$ containing $\Sigma(\bar{f}, r)$. Assume that $\tilde{N} \geq 1$ (The trivial case when $\tilde{N} = 0$ is not of interest). Let $\Gamma$ be an $(\tilde{N}-1)$-dimensional face of $\Sigma(\bar{f}, r)$ not containing the origin. Let $\hat{\Gamma}$ be the convex hull of $\Gamma \cup \{(0, 0, ..., 0)\}$. Let $\tilde{V}(\Gamma)$ (resp. $\tilde{V}(\hat{\Gamma})$) be the volume of $\Gamma$ (resp. $\hat{\Gamma}$) with respect to the Haar measure on the smallest affine space (resp. linear space) containing $\Gamma$ (resp. $\hat{\Gamma}$), normalized so that a fundamental domain for the induced lattice has volume 1. Let $D(\Gamma)$ to be the smallest positive integer such that*

$$w_\Sigma\left(\mathbb{Z}^N \cap C(\Gamma)\right) \subseteq \frac{1}{D(\Gamma)}\mathbb{Z}_{\geq 0} \cup \{+\infty\}.$$

*Then*

$$\boxed{\frac{\tilde{V}(\Gamma)D(\Gamma)}{\tilde{N}} = \tilde{V}(\hat{\Gamma})}.$$

*Proof.* We first note that it suffices to prove the equation in the case when $\Gamma$ is a simplex, for we can always triangulate the face into simplices and then add up the volumes. Also note that $\hat{\Gamma}$ is an $\tilde{N}$-dimensional simplex whenever $\Gamma$ is an $(\tilde{N}-1)$-dimensional simplicial face, not containing the origin.

We will need the following elementary fact from basic algebra.

**Lemma D.0.2.** *If $m$ is a positive integer, and $a_1, a_2, ..., a_n$ are nonzero integers, then*

$$\gcd(ma_1, ma_2, ..., ma_n) = m \cdot \gcd(a_1, a_2, ..., a_n)$$

*Proof of the lemma.* It suffices to prove for the case when $n = 2$ due to the fact that $\gcd(ma_1, ma_2, ..., ma_n) = \gcd(\gcd(ma_1, ma_2, ..., ma_{n-1}), ma_n)$.

Now, if $d = \gcd(a_1, a_2)$ and $D = \gcd(ma_1, ma_2)$, then $md \mid ma_1$ and $md \mid ma_2$, and hence, $md \mid D$. On the other hand, by Bézout's identity, there are integers $r, s$ such that $ra_1 + sa_2 = d$. Hence, $md = r(ma_1) + s(ma_2)$, and again by Bézout's identity, $md$ is a multiple of $D$. Thus, $md = D$. □

We return to proving the proposition.

Choose an orthonormal basis for $E(\bar{f})$, and express the vertices $v_1, v_2, ..., v_{\tilde{N}}$ of $\Gamma$ in terms of this basis. We may thus form the $\tilde{N} \times \tilde{N}$ matrix, $M$, whose $i$-th column has the coordinates $v_{i,j}$ of the vertex $v_i$. Let $\boxed{d = |\det(M)|}$. Then it is clear that

$$\tilde{V}(\hat{\Gamma}) = \frac{d}{\tilde{N}!}.$$

Now, let $Q$ be the $(\tilde{N} - 1) \times \tilde{N}$ matrix obtained from $M$ as

$$Q = \begin{bmatrix} \mathbf{c}_1 - \mathbf{c}_{\tilde{N}} & \mathbf{c}_2 - \mathbf{c}_{\tilde{N}} & \dots & \mathbf{c}_{\tilde{N}-1} - \mathbf{c}_{\tilde{N}} \end{bmatrix}$$

where $\mathbf{c}_i$ is the $i$-th column of $M$. For each $j = 1, 2, ..., \tilde{N}$, let $d_j$ be the $j$-th $(\tilde{N} - 1) \times (\tilde{N} - 1)$-subdeterminant of the matrix $Q$, obtained by deleting the $j$-th row. Then, by the definition of $\tilde{V}(\Gamma)$, we have that

$$\tilde{V}(\Gamma) = \frac{|\gcd(d_1, d_2, ..., d_{\tilde{N}})|}{(\tilde{N} - 1)!}.$$

For convenience, let $D$ denote $D(\Gamma)$. Then it is clear that it suffices to prove that

$$\boxed{\gcd(d_1, d_2, ..., d_{\tilde{N}}) = \frac{d}{D}}.$$

**Remark D.0.3.** When $\tilde{N} = 1$, the equation $\tilde{V}(\Gamma)D(\Gamma) = \tilde{N}\tilde{V}(\hat{\Gamma})$ holds trivially. In this case, clearly $\tilde{V}(\hat{\Gamma}) = D(\Gamma)$, and observe that $\det\ [] = 1$. Hence, we only consider $\tilde{N} > 1$ from now onwards.

Now, by the definition of $D = D(\Gamma)$, (cf. Proposition 2.2.2), there exists a linear form in $x = (x_1, x_2, ..., x_{\tilde{N}})$, namely,

$$a_1x_1 + a_2x_2 + ...a_{\tilde{N}}x_{\tilde{N}}$$

such that the hyperplane containing the face $\Gamma$ in $E(\bar{f})$ has equation

$$a_1x_1 + a_2x_2 + ...a_{\tilde{N}}x_{\tilde{N}} = D$$

with $\boxed{\gcd(a_1, a_2, ..., a_{\tilde{N}}) = 1}$. Hence, the coordinates $v_{i,j}$ of *each* of the vertices $v_i$ of $\Gamma$ satisfy

$$a_1v_{i,1} + a_2v_{i,2} + \ldots + a_{\tilde{N}}v_{i,\tilde{N}} = D$$

for $i = 1, 2, ..., \tilde{N}$.

Let $\mathbf{a} = (a_1, a_2, ..., a_{\tilde{N}})$, and let $\mathbf{D} = (D, D, ..., D)$. Thus, $\mathbf{a}$ satisfies the matrix equation,

$$M^T\mathbf{a} = \mathbf{D}.$$

On solving for the $a_j$ using Cramer's rule, we get that

$$a_j = \frac{D_j}{d}$$

where $D_j$ is the determinant of the matrix $M^T$ whose $j$-th column is replaced by the vector $\mathbf{D}$.

On evaluating the determinants $D_j$ by first subtracting the last row from each of its

first $(\tilde{N}-1)$ rows and then expanding along the $j$-th column, it is easily seen that

$$D_j = \pm D d_j$$

whence we have that

$$d_j = \pm \left(\frac{d}{D}\right) a_j$$

for each $j = 1, 2, ..., \tilde{N}$.

Finally, since $\gcd(a_1, a_2, ..., a_{\tilde{N}}) = 1$, we deduce from the above equations and from the above lemma that

$$\gcd(d_1, d_2, ..., d_{\tilde{N}}) = \frac{d}{D}.$$

□